
2025
ASA STAFFING
LAW & COMPLIANCE
CONFERENCE
MAY 8–9 ★ WASHINGTON, DC

The Threat Is Real: Combatting Fraud in the Staffing Industry

Evan Fenaroli
VP, Management and Professional Liability
Philadelphia Insurance Cos.

Kerri-Ann Griggs, Esq.
Partner
Alston & Bird

Ariel Zion, Esq.
Chief Legal Officer
Insight Global

A View From the Inside

- **The Bait and Switch**
  - Interview one person but a different person shows up for the assignment
  - How to mitigate: video interviews where possible, in-person meetings required or cameras always on

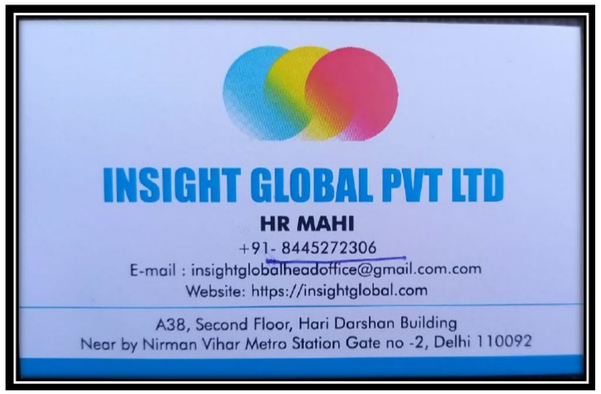
- **The Man in the Middle**
  - Email purporting to be from vendor or employee requesting change in bank account information
  - How to mitigate: train employees in payroll, human resources, and accounts payable to separately verify requests independent of original request (phone call to a known number or video call to internal employee is best); don't get comfortable with email history or threads

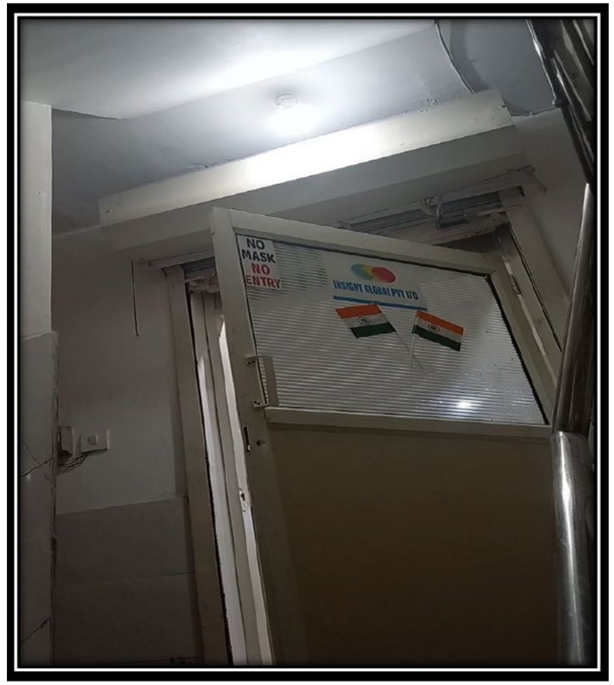
- **The Payroll Scheme ("Fake Client")**
  - Request to payroll employees providing fraudulent identity information with payment being made to bad guy's bank account
  - How to mitigate: identity fraud detection measures (software, training), bank account audits, IP address monitoring, maintain credit or background check requirements (especially for new clients), tighter invoicing deadlines

- **The Trade Dress Grifter**
  - Company posing as your company and defrauding unknowing candidates based on your goodwill
  - How to mitigate: website disclosures, hire an investigator in a foreign country to shut it down

The Real InsightGlobal

Not the Real Insight Global





Coverage for Crime and Fraud:

Crime and Fidelity Insurance

- **Employee Theft or Employee Dishonesty**
  - Theft, embezzlement of insured's money, securities, or property by employees
- **Third-Party Crime**
  - Theft, embezzlement of *client* money, securities, or property by *insured's* employees
- **Forgery and Alteration / Money Orders / Counterfeit Currency**
- **Theft of Money and Securities**
  - By an outsider or nonemployee (either inside or outside insured's premises)
- **Computer Fraud**
  - Theft of funds arising out of the fraudulent use of a computer (implies hacking or unauthorized access to a computer system)
- **Funds Transfer Fraud**
  - Bank relying on fraudulent instructions to transfer funds
- **Social Engineering Fraud or Fraudulent Impersonation**
  - Employee tricked into transferring funds under false pretenses

Coverage for Crime and Fraud:
Cyber Insurance

Coverage for Data-Related Incidents:

- **First Party Coverage for Cyber Incidents**
  - Breach response
  - Cyber extortion
  - Business interruption or income loss
  - Data restoration
- **Third-Party Liability**
  - Network security or privacy liability
  - Regulatory coverage (defense and fines or penalties)

Cyber Crime Coverage:

- **Social Engineering / Fraudulent Impersonation**
- **Invoice Manipulation**
  - Fraudulent invoices sent to insured's clients or customers (usually from compromised email account)
- **Telecommunications Fraud**
  - Fraudulent use of insured's phone or telecom systems
- **Cryptojacking**
  - Use of insured's computing resources for cryptocurrency mining

Common Insurance Claims

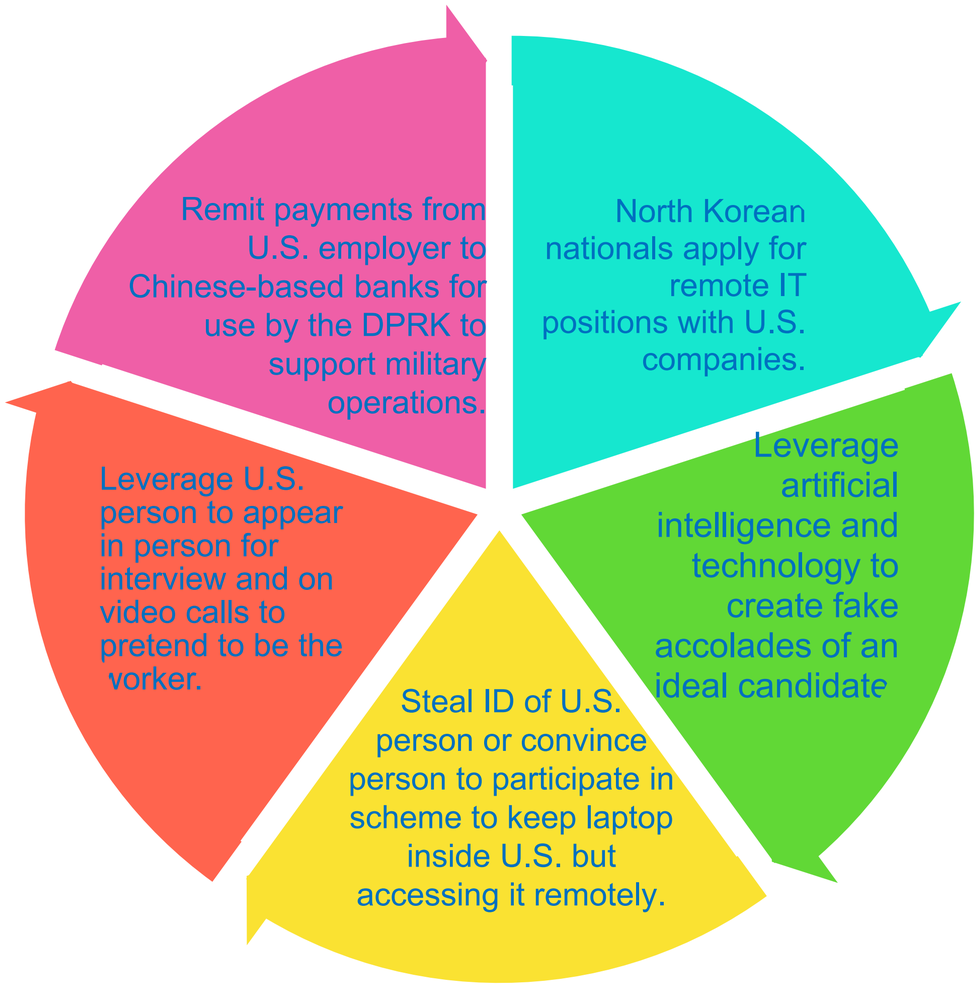
- **Time Card Fraud**
  - Falsification / forgery of signatures
  - Employee theft coverage
- **Fake Employee / Payroll Fraud**
  - Employee theft coverage
- **Social Engineering / Fraudulent Impersonation / Business Email Compromise**
  - Fake requests from vendors, clients, insurance agents, etc. to transfer funds or update bank info for future payments
- **Theft / Embezzlement of Client Funds by Staffed Employee**
  - Third-party crime coverage
- **Fake Invoices Sent to Clients From Compromised Email Account**
  - Invoice manipulation coverage
  - Other cyber coverage (breach response, etc.)
- **W2 Fraud / Social Engineering**
  - First- and third-party cyber coverage (breach response, liability to impacted employees, etc.)
- **Ransomware / Cyber Extortion**
  - First and third party cyber coverage (breach response, extortion, business income loss, regulatory defense, liability to employees/customers, etc.)

Ripped From the Headlines

- **North Korean Information Technology Worker Scheme**
  - North Korean nationals in China and Russia working for U.S. IT staffing companies under stolen identities
  - Generate millions of dollars for the benefit of North Korea; steal sensitive company information for ransom
  - "The DPRK [Democratic People's Republic of Korea] has dispatched thousands of skilled IT workers around the world, earning revenue that contributes to the North Korean regime with the aim of deceiving U.S. and other businesses worldwide" *justice.gov/archives/opa/pr/fourteen-north-korean-nationals-indicted-carrying-out-multi-year-fraudulent-information*
  - Lengths to which the scheme went:
    - Stolen identities of U.S. persons
    - Paying U.S. persons to attend job interviews or work meetings remotely under fake identities
    - Registering web domains or designing phony websites to convince prospective employers of experience or qualifications
    - Laptop "farms" in the U.S.

    But there were red flags:
    - Physical addresses listed on "business" websites were residential addresses
    - "Business" telephone numbers had area codes that did not correspond to purported location
    - Websites contained broken English

The Scheme


North Korean nationals apply for remote IT positions with U.S. companies.
Leverage artificial intelligence and technology to create fake accolades of an ideal candidate
Steal ID of U.S. person or convince person to participate in scheme to keep laptop inside U.S. but accessing it remotely.
Leverage U.S. person to appear in person for interview and on video calls to pretend to be the worker.
Remit payments from U.S. employer to Chinese-based banks for use by the DPRK to support military operations.

Ripped From the Headlines

Red Flags

- Inconsistencies in name spelling, contact information, education and work history, and social medial profiles
- Worker requests that items, such as documents or work-related equipment (laptop, mobile device, etc.), be sent to the worker at an address not previously listed on the worker's identification documentation—be leery if the worker claims they cannot receive items at the address on their identification documentation
- Worker is unable to attend requested calls or meetings during normal business hours
- Inability to reach the worker in a timely manner, especially through instant communication (on Teams, etc.)

Ripped From the Headlines

Implications:

- Disclosure to the Office of Foreign Assets Control (because you have paid a North Korean national)
- Disgorgement of funds
- Client disclosure
- Potential cybertheft of client property (check your indemnification language) and related ransom
- Reputational risk
- Time, effort, and energy of a DOJ investigation

Ripped From the Headlines

Indictments Continue:

- Dec. 12, 2024—14 North Korean nationals indicted
- Jan. 23, 2025—two North Korean nationals, one Mexican national, two U.S. nationals (accomplices) indicted

Guardrails

Employers Are Prohibited From

- Making hiring, firing, or recruiting decisions based on workers' citizenship, immigration status, or national origin
- Treating workers differently based on their workers' citizenship, immigration status, or national origin when verifying their work authorization, including during the Form I-9 and E-Verify processes
- Unfair documentary practices—requesting more or different documents from subset of workers due to their national origin, citizenship, or immigration status

Guardrails

Rule of Thumb:

- Employers should not limit hiring and recruitment based on **workers' citizenship, immigration status, or national origin unless required** by law, government contract, or executive order.

Examples of Restrictive Language

In Job Postings:

- “Only U.S. citizens”
- “Only U.S. citizens or green card holders”
- “Must present U.S. birth certificate”
- “No [nationals of a specific country]”

In Communication With Applicants:

- Are you a U.S. citizen?
- Need your green card or U.S. passport
- Only citizens allowed on this project
- Bring your U.S. driver’s license and Social Security card

Contradiction

Doesn't the statute allow discrimination sometimes?

- Allows certain citizenship restrictions when **required** by law, government contract, or executive order

What does that mean?

- The contract under which the worker is being sourced must
  (a) Require applicants to be a specific citizenship status
  (b) Contain evidence of the valid basis for the restriction (the law or executive order)

Contradiction

Obligations of Employer to Verify Validity of Restriction:

- Employers should obtain confirmation from the end client that the citizenship restriction is **required** by law, government contract, or executive order.

- **Rule of Thumb**: **Trust but verify.** Do not assume that since your end client is a government contractor, the must have a valid basis for the citizenship restriction.

Protect the Brand

Protecting the Brand While Not Discriminating:

- Have a separate security check measure.
- Require candidate interviews in person and initial onboarding and training in person *for everyone*.
- Have a fraud policy invoking punitive measures against workers who misrepresent facts about themselves to the company.
- Observe subject matter aptitude of employee in person and note any substantial variance in performance when employee works remotely.

Leverage Technology and Security Tools:

- Track location of all corporate devices. Note suspicious activity (employee lives and works in Atlanta, but log ins to the system are always registering from a different state or location). Company may leverage tools to verify if an image was created using AI.
- Require identity documents for building access **(this is separate from the Form I-9 process).** You may specify certain documents for creating a work ID with a photograph of the worker on it for building access.
- Require notarized proof of identity *for all workers* prior to employment.

Reference Links for North Korean IT Workers

Government Guidance:

May 16, 2022: *ofac.treasury.gov/media/923126/download?inline*

DOJ Press Releases:

Oct. 18, 2023: *justice.gov/archives/opa/pr/justice-department-announces-court-authorized-action-disrupt-illicit-revenue-generation*

May 16, 2024: *justice.gov/archives/opa/pr/justice-department-announces-arrest-premises-search-and-seizures-multiple-website-domains*

Aug. 8, 2024: *justice.gov/archives/opa/pr/justice-department-disrupts-north-korean-remote-it-worker-fraud-schemes-through-charges-and*

Jan. 23, 2025: *justice.gov/opa/pr/two-north-korean-nationals-and-three-facilitators-indicted-multi-year-fraudulent-remote*