The Banking Law Journal

Established 1889

An A.S. Pratt™ PUBLICATION **SEPTEMBER 2022**

LexisNexis

THE BANKING LAW JOURNAL

VOLUME 139 **NUMBER 8** **September 2022**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call:

Matthew T. Burke at ..... (800) 252-9257
Email: ..... matthew.t.burke@lexisnexis.com
Outside the United States and Canada, please call . . . . . (973) 820-2000

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3385
Fax Number . . . . . (800) 828-8341
Customer Service Website . . . . . http://www.lexisnexis.com/custserv/

For information on other Matthew Bender publications, please call

Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (937) 247-0293

ISBN: 978-0-7698-7878-2 (print)
ISSN: 0005-5506 (Print)

Cite this publication as:

The Banking Law Journal (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.

Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW BENDER

(2022–Pub.4815)

Editor-in-Chief, Editor & Board of Editors

THE BANKING LAW JOURNAL (ISBN 978-0-76987-878-2) (USPS 003-160) is published ten times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquiries and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to bankers, officers of financial institutions, and their attorneys. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL, LexisNexis Matthew Bender, 230 Park Ave, 7th Floor, New York, NY 10169.

POSTMASTER: Send address changes to THE BANKING LAW JOURNAL, A.S. Pratt & Sons, 805 Fifteenth Street, NW, Third Floor, Washington, DC 20005-2207.

U.S. Issues Guidance to Companies Warning of Cybersecurity and Sanctions Risks Posed by IT Workers Directed by North Korea

By Kevin E. Gaunt, Ryan A. Glasgow, Sevren R. Gourley, Michael La Marca, William L. Newton and Aaron P. Simpson*

The North Korean government dispatches thousands of its highly skilled IT workers around the world to generate revenue necessary to fund its weapons programs in violation of U.S. sanctions. This creates cybersecurity and sanctions risk exposure for companies engaging or contracting with remote IT personnel. The authors of this article discuss the risks and mitigation strategies.

The U.S. Department of State, U.S. Department of Treasury, and the Federal Bureau of Investigation ("FBI") issued combined guidance ("IT Workers Advisory") on efforts by North Korean nationals to secure freelance engagements as remote information technology ("IT") workers by posing as non-North Korea nationals. The IT Workers Advisory provides employers with detailed information on how North Korean IT workers operate, highlights red flag indicators for companies hiring freelance developers and for freelance and payment platforms to identify these workers, and provides general mitigation measures for companies to better protect against inadvertently engaging these workers or facilitating the operations of the North Korean government in violation of U.S. sanctions.

BOTTOM LINE

The North Korean government ("DPRK") dispatches thousands of highly skilled North Korean IT workers around the world to generate revenue necessary to fund its weapons programs in violation of U.S. sanctions. This creates cybersecurity and sanctions risk exposure for companies engaging or contracting with remote IT personnel. Companies can mitigate these risks by incorporating diligence for red flag indicators of North Korean nationals into cybersecurity and sanctions compliance programs.

THE FULL STORY

The IT Workers Advisory follows a 2021 United Nations ("UN") panel report studying the scope of North Korea's use of IT workers to earn foreign

* Kevin E. Gaunt (kgaunt@huntonak.com), Ryan A. Glasgow (rglasgow@huntonak.com), Sevren R. Gourley (sgourley@huntonak.com), Michael La Marca (mlamarca@huntonak.com), William L. Newton (wnewton@huntonak.com) and Aaron P. Simpson (asimpson@huntonak.com) are attorneys at Hunton Andrews Kurth LLP.

currency and its methods for evading employer due diligence efforts and know-your-customer/anti-money laundering protocols. The UN panel concluded that DPRK IT workers use several methods to obtain freelance IT work without revealing their identity, including by setting up accounts on freelance developer platforms with unwitting clients around the world, especially in China, Russia, Ukraine, Serbia, Canada and the United States.

The IT Workers Advisory warns companies that DPRK IT workers specifically target freelance contract opportunities from employers located in wealthier nations, including those in North America, Europe and East Asia. In many cases, DPRK IT workers present themselves as South Korean, Chinese, Japanese, or Eastern European, and U.S.-based teleworkers. In some cases, DPRK IT workers further obfuscate their identities by creating arrangements with third-party sub-contractors. These sub-contractors are non-North Korean, freelance IT workers who complete contracts for the DPRK IT workers. DPRK IT managers have also hired their own teams of non-North Korean IT workers who are often unaware of the real identity of their North Korean employer or the fact that their employer is a DPRK company. The DPRK IT managers use their outsourced employees to make software purchases and interact with customers in situations that might otherwise expose a DPRK IT worker.

RISKS TO COMPANIES

DPRK IT workers present a number of risks to companies that engage or contract with remote IT personnel, particularly those directly or indirectly engaging IT workers through freelance platforms:

Cybersecurity Risks

The IT Workers Advisory warns that, although DPRK IT workers normally engage in non-malicious IT work, such as the development of a virtual currency exchange or a website, DPRK IT workers have used the privileged access gained as contractors to enable DPRK's malicious cyber activity. Some overseas-based DPRK IT workers have also provided logistical support to DPRK-based malicious cyber actors, although the IT workers are unlikely to be involved in malicious cyber activities themselves. DPRK IT workers may share access to virtual infrastructure, facilitate sales of data stolen by DPRK cyber actors, or assist with the DPRK's money-laundering and virtual currency transfers. DPRK IT workers have also assisted DPRK officials in procuring WMD and ballistic missile-related items for the DPRK's prohibited weapons programs.

Sanctions Risks

The Department of the Treasury's Office of Foreign Assets Control ("OFAC") administers the U.S. sanctions against North Korea. Under this sanctions

program, U.S. persons are prohibited from engaging in significant activities on behalf of DPRK, including activities that undermine cybersecurity or other malicious cyber-enabled activities, import from or export to North Korea any goods, services, or technology; sell, supply, transfer, or purchase (directly or indirectly), to or from North Korea or any person acting for or on behalf of DPRK, any software, or materially assist, sponsor or provide financial, material, or technological support for, or goods or services to or in support of, DPRK.

OFAC-administered sanctions are enforced on a strict liability basis. However, penalties for sanctions violations may be reduced for companies that conduct reasonable diligence as part of a sanctions compliance program. OFAC has issued guidance on what it terms a "risk-based approach" to sanctions compliance that advises companies to consider known risks in their business operations when designing and implementing a sanctions compliance program.

Following the IT Workers Advisory, companies should consider the engagement of remote IT services, particularly through freelance platforms, as a potential point of sanctions exposure and update compliance programs accordingly consistent with OFAC's guidance.

MITIGATION STRATEGIES

DPRK IT Worker Obfuscation Techniques

The IT Workers Advisory warns of a number of specific techniques used by DPRK IT workers. Specifically, that DPRK IT workers deliberately obfuscate their identities, locations, and nationality online, often using non-Korean names as aliases, making it difficult for employers to identify them. They will also use virtual private networks ("VPNs"), virtual private servers ("VPSs"), or utilize third-country IP addresses to appear as though they are connecting to the internet from inconspicuous locations and reduce the likelihood of scrutiny of their DPRK location or relationships. DPRK IT workers can rely on the anonymity of telework arrangements, use proxies for account creation and maintenance, and favor the use of intermediaries and communications through text-based chat instead of video calls.

The IT Workers Advisory also warns that DPRK IT workers use proxy accounts to bid on, win, work on, and get paid for projects on freelance software developer websites. These proxy accounts may belong to third-party individuals, some of whom sell their identification and account information to the DPRK IT workers. In some cases, DPRK IT workers pay fees to these individuals for use of their legitimate platform accounts. DPRK IT workers may populate freelance platform profiles with the real affiliations, references, and work experience of the proxy.

At times, DPRK IT workers engage other non-North Korean freelance workers on platforms to propose collaboration on development projects. DPRK IT workers can take advantage of these business relationships to gain access to new contracts and virtual currency accounts used to conduct IT work over United States or European virtual infrastructure. Hiding their real locations allows DPRK IT workers to violate terms of service agreements for the online platforms and services they use to provide freelance IT work. As part of their tradecraft, DPRK IT workers may also use single, dedicated devices for each of their accounts, especially for banking services, to evade detection by fraud prevention, sanctions compliance and anti-money laundering measures.

DPRK IT workers routinely use counterfeit, altered, or falsified documents, including identification documents, and forged signatures—either that they have made themselves using software such as Photoshop, or that they have paid a document forgery company to alter, combining the IT worker's own or a provided photo with the identifying information of a real person.

Red Flags

The IT Workers Advisory sets forth a number of "red flags" that may be indications that DPRK IT workers are using freelance work or payment platforms, including:

- Multiple logins into one account from various IP addresses in a relatively short period of time, especially if the IP addresses are associated with different countries, logins into multiple accounts on the same platform from one IP address, or logins into one account continuously for one or more days at a time;
- Router port or other technical configurations associated with use of remote desktop sharing software, such as port 3389 in the router used to access the account, particularly if usage of remote desktop sharing software is not standard company practice;
- Frequent use of document templates for things such as bidding documents and project communication methods, especially the same templates being used across different developer accounts;
- Frequent transfers of money through payment platforms, especially to bank accounts in China, and sometimes routed through one or more companies to disguise the ultimate destination of the funds;
- Use of digital payment services, especially China-linked services;
- Seeking payment in virtual currency in an effort to avoid the formal financial system;
- Inconsistencies in name spelling, nationality, claimed work location,

contact information, educational history, work history, and other details across a developer's freelance platform profiles, social media profiles, external portfolio websites, payment platform profiles, and assessed location and hours;

- Surprisingly simple portfolio websites, social media profiles, or developer profiles;
- Direct messaging or cold-calls from individuals purporting to be C-suite level executives of software development companies to solicit services or advertise proficiencies;
- Receipt of items at an address not listed on the developer's identification documentation (be particularly suspicious if a developer claims they cannot receive items at the address on their identification documentation);
- Requesting payment for contracts without meeting production benchmarks or check-in meetings;
- Inability to conduct business during required business hours;
- Incorrect or changing contact information, specifically phone numbers and emails, or biographical information which does not appear to match; and
- Failure to complete tasks in a timely manner or to respond to tasks or inability to reach them in a timely manner, especially through "instant" communication methods.

Mitigation

The IT Worker Advisory provides the following risk mitigation strategies for employers:

- Conduct video interviews to verify a potential freelance worker's identity;
- Conduct a pre-employment background check, drug test, and fingerprint/biometric log-in to verify identity and claimed location;
- Avoid payments in virtual currency and require verification of banking information corresponding to other identifying documents;
- Use extra caution when interacting with freelance developers through remote collaboration applications, such as remote desktop applications;
- Consider disabling remote collaboration applications on any computer supplied to a freelance developer;
- Verify employment and higher education history directly with the listed

companies and educational institutions, using contact information identified through a search engine or other business database, not directly obtained from the potential freelance worker or from their profile;

- Check that the name spelling, nationality, claimed location, contact information, educational history, work history, and other details of a potential hire are consistent across the developer's freelance platform profiles, social media profiles, external portfolio websites, payment platform accounts, and assessed location and hours of work (be extra cautious of simple portfolio websites, social media profiles, or developer profiles);
- Be cautious of a developer requesting to communicate on a separate platform outside the original freelance platform website where a company initially found the IT worker;
- If sending to a developer documents or work-related equipment such as a laptop, only send to the address listed on the developer's identification documents and obtain additional documentation if the developer requests that the laptop or other items be sent to an unfamiliar address (be suspicious if a developer cannot receive items at the address on their identification documentation); and
- Be vigilant for unauthorized, small-scale transactions that may be fraudulently conducted by contracted IT workers (in one case cited by the IT Workers Advisory, DPRK IT workers engaged as developers by a U.S. company fraudulently charged the U.S. company's payment account and stole over $50,000 in 30 small installments over a matter of months. The U.S. company was not aware the developers were North Korean or of the ongoing theft activity due to the slight amounts).

U.S. companies engaging or contracting with remote IT workers, particularly through freelance IT worker platforms, should consider the cybersecurity and sanctions exposure presented by DRPK IT worker activity carefully and take steps to mitigate risks through a sanctions compliance program. Non-U.S. individuals and companies should also be aware of this issue, as well as OFAC's authority to sanction non-U.S. persons engaged in certain prohibited activities or to take enforcement action against non-U.S. persons who cause or conspire to cause a U.S. person to violate U.S. sanctions. Violations of U.S. sanctions may result in significant civil or criminal penalties as well as reputational harm.