AN A.S. PRATT PUBLICATION
SEPTEMBER 2026
VOL. 12 NO. 7

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 12 **NUMBER 7** **September 2026**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at ..... (908) 673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
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
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2026–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine 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 inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. 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 opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, the editor(s), RELX, LexisNexis, Matthew Bender & Co., Inc, or any of its or their respective affiliates.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Drift Protocol Exploit: Why "Social Trust" Is the Newest Cybersecurity Gap

By Rajeev Raghavan, Anand Sithian and Sarah Rippy*

In this article, the authors explain that a $285 million theft from a decentralized perpetual futures exchange on the Solana blockchain serves as a high-stakes reminder that the human element remains one of the biggest cybersecurity gaps in any organization.

The $285 million theft from Drift Protocol serves as a high-stakes reminder that the human element remains one of the biggest cybersecurity gaps in any organization. This was not a "hack" in the traditional sense of breaking through a digital wallet. North Korean actors used sophisticated social engineering to exploit human trust – highlighting what looks like a "hacking" risk into valuable lessons learned for cybersecurity oversight.

BACKGROUND

On April 1, 2026, Drift Protocol, a decentralized perpetual futures exchange on the Solana blockchain, suffered a security incident resulting in the theft of approximately $285 million in digital assets. Drift subsequently attributed[1] the operation to UNC4736, a North Korean state-affiliated group also tracked as AppleJeus or Citrine Sleet.

Mandiant previously attributed[2] the October 2024 Radiant Capital hack to UNC4736 – in which threat actors stole approximately $50 million using a similar social engineering approach, posing as a known contact and delivering malware through a file shared via a messaging platform.

WHAT MAKES THE DRIFT EXPLOIT UNIQUE

The Drift attack combined a sustained social engineering campaign with technical exploitation. The threat actors began cultivating in-person relationships with Drift personnel in fall 2025, presenting themselves as a legitimate quantitative trading firm. Over the following months, they attended major industry conferences in person, participated in working sessions, helped fix minor issues, and deposited over $1 million of their own capital into the platform – building the kind of trust that makes their eventual requests appear routine.

The technical compromise was equally deliberate and unfolded in three stages.

---

* The authors, attorneys with Crowell & Moring LLP, may be contacted at rraghavan@crowell.com, asithian@crowell.com and srippy@crowell.com, respectively.

[1] https://x.com/VelocityDEX/status/2040611161121370409.

[2] https://medium.com/@RadiantCapital/radiant-capital-incident-update-e56d8c23829e.

Stage 1 - Device and credential compromise

The threat actors exploited a vulnerability to execute malicious code and distributed that code using a legitimate app store.

Stage 2 - Obtaining administrative control

The threat actors exploited Solana's "durable nonces"[3] feature – which allows transactions to be signed in advance and executed later and thus remain valid indefinitely, unlike standard Solana transactions that expire after roughly 90 seconds. Drift's protocol was governed by a "Security Council" – a small group of trusted individuals (five in Drift's case) – who held signing privileges and any action required at least two members to approve. Using social engineering, the threat actors induced two members[4] to unwittingly pre-sign transactions transferring administrative control of the platform.

Stage 3 - Draining funds

With administrative control obtained, the threat actors introduced a fake token as collateral, artificially inflated its value through wash trading, and used that manufactured position to withdraw substantial quantities of legitimate tokens. Because Drift is configured for instant execution, there was no emergency brake once the drain began – a process they completed within minutes, with laundering operations continuing for several hours thereafter. Stolen assets were then rapidly converted into stablecoins, bridged across blockchain networks, and reconverted into more liquid assets. At least 20 other protocols report disruptions or losses as a result.

FAMILIAR PATTERN OF DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA (DPRK) ACTORS

The Drift incident fits within a sustained pattern of North Korea-linked financial crime. DPRK nationals frequently pose as IT professionals to infiltrate U.S. companies as remote workers, including in the digital assets sector, sometimes using deepfake technology. The underlying methods are strikingly similar in both contexts: sustained efforts to appear legitimate, deceptive identities, trust-building over time, access acquisition, and rapid monetization. The U.S. Department of Justice (DOJ) has made this convergence explicit in prior enforcement actions, noting that North Korean remote IT workers have used insider access to steal funds, exfiltrate proprietary information, or extort victim organizations.

According to Drift, the individuals who appeared in person at industry conferences leading up to the Drift exploit did not have the hallmarks of North Korean operatives. DPRK-linked operations at this level of sophistication routinely deploy third-party

[3] https://www.coindesk.com/tech/2026/04/02/how-a-solana-feature-designed-for-convenience-let-an-attacker-drain-usd270-million-from-drift.

[4] https://www.chainalysis.com/blog/lessons-from-the-drift-hack/.

intermediaries with fully constructed professional identities, employment histories, and public-facing credentials, usually fictitious, designed to withstand due diligence.

U.S. authorities have publicly attributed[5] billions of dollars in cryptocurrency theft to North Korean actors, with proceeds assessed to support the regime's missile and nuclear weapons programs. The U.S. Department of the Treasury's Office of Foreign Assets Control's (OFAC) March 2026 sanctions announcement[6] further described North Korea's remote IT worker schemes as a meaningful source of revenue for those programs. The same tactics are being applied across technology and other sectors that rely on remote workers, contractors, or lean approval structures.

POTENTIAL MITIGATION MEASURES

The Drift incident is a reminder for companies – across sectors – to remain vigilant to both remote worker IT scams and in-person initiated exploits. Companies should consider the following:

- *Treat high-risk approvals as a security control.* Ensure personnel responsible for significant financial or administrative actions have complete, independently verified information about what they are authorizing before acting. Approval processes that depend primarily on familiarity or trust are vulnerable to the kind of manipulation that impacted Drift.

- *Implement mandatory "cooling-off" periods.* Where possible, adjust transaction processes to prevent major financial or administrative events from executing instantly (e.g., circuit breakers). A mandatory 24-, 48- or 72-hour delay between approval and execution allows security teams to review and, if necessary, halt suspicious activity.

- *Reassess privileged access and concentration risk.* Identify where a small number of approvals can produce outsized consequences. Companies should assess low threshold quorums for social engineering risks and consider multi-signature (multisig) or multiple approver thresholds where a majority (*e.g.,* 3 of 5, 4 of 7) of signatures or approvals are required, adding redundancies into approval processes.

- *Treat hiring and contractor onboarding as part of the security perimeter.* HR and security functions should work cooperatively and avoid operating in silos. Implement robust identity verification at onboarding and maintain it throughout the engagement, treating behavioral red flags as escalation triggers. New York State Department of Financial Services guidance,[7]

[5] https://www.justice.gov/archives/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

[6] https://home.treasury.gov/news/press-releases/sb0416.

[7] https://www.dfs.ny.gov/industry-guidance/industry-letters/il20241101-cyber-advisory-remote-workers-nk.

which applies to certain major banks, FinTechs, and crypto companies, recommends requiring video verification during hiring to help guard against identity concealment and deepfake risk.

- *Apply zero-trust contributor vetting.* Treat every external contributor – regardless of tenure or how they were introduced – with a zero-trust mindset. Code reviews and transaction audits should be performed by security teams or independent third parties.

- *Integrate legal, compliance, security, and incident response functions.* Pre-establish escalation paths and coordinated response protocols. Pre-emptively work with experienced cybersecurity counsel to conduct tabletops and be prepared to quickly activate counsel, incident response firms, and PR firms in the event of an incident.

- *Evaluate sanctions exposure proactively.* Assess whether screening and monitoring procedures are calibrated to the risk of inadvertently handling proceeds linked to sanctioned actors. Consider counsel with deep law enforcement contacts at the Federal Bureau of Investigation (FBI), DOJ, and other agencies who can quickly issue freeze letters or obtain seizure orders to prevent further asset dissipation.

IN SUMMARY

- Threat actors are no longer just looking for software bugs; they are spending months building fake identities to "befriend" organizations and conduct corporate espionage.

- The Drift incident reflects a familiar DPRK playbook with an in-person twist: identity deception, relationship-building, privileged access, and rapid monetization – the same methods central to North Korea's remote IT worker schemes.

- Where a small group of individuals can authorize consequential financial or administrative actions, social engineering and insider-enabled compromise present significant legal, compliance, and operational risk. High-risk approvals, access governance, and hiring controls should be treated as core security measures.