

STRIDER FOR FINTECH & DIGITAL ASSET COMPANIES

Protecting Payment Systems, Crypto Infrastructure, and High-Trust Personnel from Insider and Nation-State Threats.

Overview

Fintech companies operate in one of the fastest-moving and most targeted sectors in the world. Payment platforms, digital wallets, and crypto-processing environments hold high-value data and assets sought by state-sponsored actors, fraud networks, and proxy workers. Rapid hiring, globally distributed teams, and reliance on third-party infrastructure further expand exposure.

Strider equips CISOs, Fraud and FinCrime leaders, Global Investigations teams, and HR with intelligence on personnel, suppliers, and malicious communications—empowering fintech organizations to secure their crown-jewel payment systems and operate with confidence.

Fintech & Digital Asset Leaders Use Strider to:

- Screen applicants and remote workers for fraudulent identities or ties to state-sponsored programs.
- Prevent DPRK proxy workers and fraudulent IT hires from infiltrating engineering teams.
- Detect malicious recruitment targeting fraud, FinCrime, wallet-security, or other high-risk teams.

With Strider, fintech companies can secure their payment ecosystems, reduce fraud exposure, and protect user trust in highly targeted digital environments.



What's at Stake

Real-world incidents reveal how payment systems, digital wallets, and crypto infrastructure are actively targeted by nation-state actors.

- **DPRK Proxy Workers Penetrating U.S. Crypto & Fintech Firms (2023)**¹: North Korean operatives have repeatedly used falsified identities to infiltrate IT and engineering teams, directly targeting payment infrastructure and crypto rails.
- **Insider-Enabled Breach at a Major Crypto Exchange (2024-2025)**²: Coinbase disclosed that rogue overseas support contractors, bribed by cybercriminals, exfiltrated sensitive customer data and attempted a \$20M ransom which affected tens of thousands of users.
- **Crypto Processing Executive Linked to Illicit Foreign Activity (2023)**^{3, 4}: Recent cases, including Bitzlato CEO arrest and the JPEX exchange scandal, demonstrate how undisclosed foreign control and executive-level misconduct can expose fintech platforms to sanctions risk, money-laundering activity, and reputational damage.

¹ <https://www.techradar.com/pro/security/north-korean-fake-worker-scheme-caught-live-on-camera>

² <https://www.securityweek.com/coinbase-rejects-20m-ransom-after-rogue-contractors-bribed-to-leak-customer-data/>






³ <https://www.bloomberg.com/news/articles/2023-09-19/hong-kong-s-crypto-push-gets-blunt-warning-as-probe-erupts>

⁴ <https://www.reuters.com/technology/co-founder-seized-crypto-exchange-bitzlato-plead-guilty-us-2023-12-06/>

Failure to Act Can Lead to:

- **Loss of Customer Funds or Digital Assets:** through infiltration of engineering or fraud teams by DPRK proxy workers or high-risk contractors.
- **Regulatory Exposure & Sanctions Violations:** as hidden foreign ties in crypto-processing centers or liquidity partners trigger OFAC, DOJ, or international enforcement.
- **Infiltration of Critical Payment or Blockchain Systems:** allowing foreign-linked developers or fraudulent IT hires to compromise wallet infrastructure, smart contracts, or transaction engines.
- **Erosion of User Trust & Brand Damage:** following high-visibility incidents involving insider exploitation, unauthorized transfers, or compromised payment rails.
- **Long-Term Platform Instability:** caused by risky OSS dependencies, foreign-linked contributors, or compromised nodes that undermine security and reliability.

What Strider Does for Fintech & Digital Asset Companies

CAPABILITY	HOW IT HELPS	STRIDER PRODUCTS IN ACTION
Falsified Resume & Remote Worker Screening	Identify DPRK and other risky proxy workers, fraudulent IT hires, and falsified identities before access is granted.	 People Search & Falsified Resume Screening Automate resume checks via ATS integration; flag hidden affiliations and fake personas.
Protection of Payment Rails & Crown Jewel Systems	Safeguard high-value environments such as crypto wallets, payment engines, and settlement systems.	 Insights Surface personnel with risky ties relevant to fraud, cyber, or state-sponsored exploitation.
Crypto Processing & Vendor Risk Visibility	Vet third-party processing centers, liquidity partners, and infrastructure providers for foreign control or hidden ownership.	 Organizations Search Map multi-tier ownership, shareholders, and supply-chain dependencies.
Threat Detection & Fraud Intelligence	Detect malicious communications targeting FinCrime, trust & safety, and security teams.	 Shield Ingest high-risk domains and multilingual keywords into your SIEM/DLP to flag dangerous outreach.
Blockchain & OSS Supply-Chain Risk	Protect blockchain, smart contract, or wallet infrastructure from risky OSS contributors.	 OSS Search Identify foreign-linked contributors in blockchain tooling and dependencies.

Ready to Safeguard Your Payment Ecosystem & Digital Assets?

Schedule a demo to see how Strider helps fintech leaders prevent fraudulent hires, secure payment infrastructure, and mitigate geopolitical risk.

[REQUEST A DEMO](#) →

