

STRIDER FOR FINANCIAL SERVICES

Protecting Financial Operations, Personnel, and Critical Data from Nation-State Threats.

Overview

Financial institutions sit at the center of global capital flows, regulatory scrutiny, and geopolitical competition making their systems, people, and partnerships persistent targets for state-sponsored actors. From high-trust personnel in cybersecurity and fraud units to global counterparty relationships, financial organizations face risks that traditional security tools cannot detect.

Strider equips CISOs, Insider Threat teams, fraud leaders, and compliance organizations with visibility into personnel risk, third-party exposure, and malicious communications—empowering financial institutions to safeguard sensitive data, protect clients, and maintain operational resilience across complex, distributed environments.

Financial Services Leaders Use Strider to:

- Screen applicants, employees, vendors, and contractors for risky affiliations or falsified resumes.
- Protect high-trust teams in cybersecurity, fraud, and money-movement operations.
- Identify hidden ties, foreign control, and sanctions exposure in counterparties, customers, and global partners.
- Detect malicious outreach tied to cyber operators, economic statecraft programs, or recruitment activity.
- Equip Fraud, Insider Threat, and Compliance teams with contextual intelligence on high-risk individuals.
- Strengthen governance by identifying geopolitical exposure across personnel, partners, and global operations.

With Strider, financial institutions can protect customer trust, secure operational systems, and stay ahead of geopolitical, insider, and compliance risk.



What's at Stake

Recent incidents show how insider threats, opaque partnerships, and geopolitical pressure expose even the most established financial institutions.

- **JP Morgan & Bank of America Subpoenaed Over CATL IPO (2025)¹:** A U.S. House committee subpoenaed both banks over high-risk ties linked to a foreign entity's IPO showing how dealmaking can trigger sanctions and national-security scrutiny.
- **Wells Fargo Employee Barred from Leaving China (2025)²:** A Wells Fargo employee was prevented from exiting China during a dispute, underscoring how geopolitical leverage can directly affect financial institution personnel abroad.
- **North Korean IT Worker Scheme Targeting U.S. Companies (2023)³:** The DOJ charged DPRK operatives who used fake identities to secure jobs in U.S. firms, exposing weaknesses in personnel screening across finance and IT. Their operations have also helped North Korea steal over \$6 billion in cryptocurrency.

Failure to Act Can Lead to:

- **Regulatory & Geopolitical Scrutiny:** including sanctions exposure (OFAC), cross-border investigations, and heightened oversight from regulators and congressional committees.
- **Insider-Driven Financial Loss or Data Exposure:** as fraudulent or foreign-linked employees gain access to payment systems, customer data, or internal fraud controls.
- **Counterparty & Third-Party Failures:** resulting from hidden foreign ownership or sanctions-linked partners that jeopardize compliance and customer trust.
- **Compromised Hiring Pipelines:** allowing DPRK proxy workers or high-risk applicants to enter IT, fraud, or cybersecurity roles through falsified credentials.

What Strider Does for Financial Services

CAPABILITY	HOW IT HELPS	STRIDER PRODUCTS IN ACTION
Continuous Employee & Candidate Vetting	Verify identities, detect falsified resumes, and uncover risky affiliations before hire; especially for remote IT, cybersecurity, and R&D roles.	 People Search, & Falsified Resume Screening Automate screening through ATS integrations; identify DPRK or PRC-linked applicants attempting to impersonate Western talent.
Protection of AI, Quantum, and Cyber R&D Programs	Identify employees working on targeted technologies and provide tailored briefings to reduce recruitment risk.	 Insights (Technologies Tab) Surface targeted technologies and associated employees most at risk from state-sponsored actors.
Strategic Deal & Partner Due Diligence	Protect M&A, investment banking, and strategic transactions by identifying foreign ownership, sanctions exposure, and hidden affiliations.	 Organizations Search Map multi-tier ownership and personnel ties for deal counterparties, investors, and joint-venture partners.
Threat Intelligence for High-Risk Outreach	Detect malicious emails, domains, and multilingual terms tied to state-sponsored cyber or recruitment activity.	 Shield Feed curated selectors into SIEM/DLP tools to identify, flag, and monitor geopolitical threats targeting employees.
Open-Source Software & Contributor Risk	Assess contributors and dependencies in open-source tooling used in internal platforms or quantitative systems.	 OSS Search Detect state-linked contributors across open-source repos; prevent supply-chain compromise.

Ready to Protect Your People, Technology, & Global Operations?

Schedule a demo to see how Strider helps enterprise financial institutions safeguard innovation, mitigate insider and geopolitical risk, and strengthen compliance across global operations.

[REQUEST A DEMO](#) →

