CLOUDGUARD
Security Done Different

Security. Done Different.

Financial Services & Insurance

Global Threat Intelligence – Q1 2026

Document version 2.2

16/03/2026

Classification: Unclassified

Executive Summary

The UK Financial Services, Insurance and private investor sector faces its highest threat level recorded by CloudGuard Intelligence since monitoring began.

The March 2026 assessment returns an overall threat **score of 84/100,** a 10-point increase from February, driven by a convergence of nation-state escalations, industrialisation of automation threat actor reconnaissance activities, surging credential theft activity on dark web markets, a wave of targeted attacks against wealth management and advisory firms globally, and elevated **FCA** and **ICO** enforcement following significant operational incidents.

Four distinct threat streams are operating simultaneously against this sector this month:

1. Financially motivated ransomware and data extortion groups (primarily DragonForce and Scattered Spider affiliates);
2. Iranian state-aligned hacktivist groups executing DDoS and mass automated vulnerability rapid exploitation campaigns against UK financial infrastructure;
3. North Korean state-sponsored actors specifically targeting UK-based cryptoasset firms and private investor platforms;
4. AI-enhanced phishing, deepfake partner impersonation, and infostealer malware are the primary delivery mechanisms across all streams.

The regulatory environment is simultaneously changing. The **FCA's** new operational incident reporting regime (in consultation since late 2024) is expected to be finalised in Q2 2026, significantly expanding disclosure obligations.

The ICO continues active enforcement against firms with inadequate controls around personal data exposed in incidents. Firms that cannot demonstrate operational resilience through documented evidence, detection telemetry, incident timelines, remediation records, face compounding regulatory and reputational exposure.

The **EU AI Act** will also feature significantly in the plans for Financial Services organisations now scaling out AI led cost and service optimisation strategies with highly innovative AI first solutions.

CLOUDGUARD

UK Financial Services & Private Investor

Cyber Threat Intelligence

Q1 2026 | Quarterly Intelligence Report

—

Threat intelligence | Dark web insights | Regulatory incidents

Sector leakage | Active threat actor tracking

Prepared by CloudGuard Threat Intelligence Unit

THREAT LEVEL

CRITICAL

Financial Services & Private Investors

Score: 84/100

▲ +10 pts vs Feb 2026

Security Done Different

Overall threat score	Active threat groups	Dark web credentials	FCA incidents (2025)
84/100	**11**	**2.1bn+**	**294**
CRITICAL	Targeting UK finance	Leaked in 2025	187 cyber-attributed

Threat landscape — Q1 2026

The UK financial sector is the single most targeted industry vertical in the country's cyber threat landscape, accounting for approximately **28%** of all UK cyber-attacks. In Q1 2025 alone, more than **70%** of London financial institutions reported attempted breaches, a figure CloudGuard Intelligence assesses as likely to have increased further through the first quarter of 2026. Three macro-level threat drivers are shaping this month's threat picture.

1. Nation-state and state-aligned threat actors

NCSC Active Alert — January 2026

On 19 January 2026, the NCSC issued a formal alert confirming persistent targeting of UK organisations by Russian state-aligned hacktivist groups. The NCSC handled 204 nationally significant cyber-attacks in 2025, more than double the 89 incidents from 2024. This represents **four major** attacks hitting UK organisations every week.

Russia (GRU/SVR affiliated groups and aligned hacktivists), China (multiple APT groups), Iran, and North Korea represent the four primary nation-state threat actors assessed by NCSC as targeting UK interests. Their relevance to the financial sector differs by actor:

- **Russian-aligned hacktivist groups** (NoName057(16), Cyber Army of Russia Reborn, Z-Pentest) are executing DDoS campaigns against UK financial infrastructure, payment platforms, and investment portals. Attacks are typically ideologically motivated, retaliation for UK policy on Ukraine, and are escalating in frequency and sophistication. Many of these are now **NCSC** explicitly warned in January 2026 that these groups are moving beyond website disruption toward operational technology targeting. Active vulnerability exploitation of zero day (many firewall technology stacks) are leveraging AI generative automation from Censys fields to escalate attack vectors from reconnaissance in minutes and hours from identification.
- **North Korean state-sponsored actors** (Lazarus Group and affiliated units) are specifically targeting UK-based cryptoasset firms and private investor platforms. NCSC confirmed in its 2025 Annual Review that UK cryptoasset firms are currently at risk of DPRK-linked hackers seeking to steal funds. Additionally, DPRK IT workers disguised as freelance contractors are almost certainly operating within UK financial services firms, creating insider threat risks.
- **Chinese APT groups** are conducting long-term espionage operations against UK financial institutions holding data on high-net-worth individuals, M&A activity, and government-related investment flows. These intrusions prioritise persistence and data exfiltration over disruption. APT10 (also known as Stone Panda, MenuPass, Red Apollo, Cloud Hopper and POTASSIUM) has specifically increased focus on MSP's supporting Financial Services, Wealth Management platforms and Private Equity companies. UNC5221 has continued to focus critical and high severity network and VPN vulnerability exploitations specifically for no day entities. APT41 (also known as Brass Typhoon, Wicked Panda, BARIUM and Double Dragon) has been the most active in detailed reconnaissance and new strain of malware TTP's.
- **Ransomware groups** with various affiliations and tactical geopolitical alignment (DragonForce, Scattered Spider affiliates) are primarily financially motivated to execute identified exploitation paths of new TTP strains giving them de facto operational freedom.

2. Financially motivated criminal threat actors

Ransomware remains the most acute and pervasive threat to UK financial organisations in 2026. Sophos data indicates **65%** of financial services organisations were hit by ransomware in 2024, the highest rate since tracking began, and **49%** had data successfully encrypted. Ransomware groups have evolved their tactics in two critical ways that elevate risk specifically for financial and investor firms:

- Extortion without encryption: groups increasingly **exfiltrate/steal data** smaller quantities of data and seek a dark settlement. The continual threat to publish (alternative TTP) without deploying encryption. This is solely evading NCSC involvement and FCA reporting particularly damaging for firms holding sensitive client financial planning data, HNW client portfolios, and personal KYC records.

- Typical settlements are within **14 days** and usually involve a dual monetisation TTP where the attack format is resold to another affiliate and repeated or mimicked within 180 days.
- Targeted timing: threat actors are now conducting **reconnaissance** over weeks or months before activating payloads, timing attacks to coincide with high-value transaction periods, M&A activity, annual reporting cycles, or regulatory submission deadlines to maximise leverage and demand compliance. There is now specific focus towards advisory firms.
- **Wealth management and RIA targeting**: ShinyHunters claimed in February 2026 to have stolen five million records from Mercer Advisors and over 100,000 from Beacon Pointe Advisors (US-based but instructive for UK equivalents). Edelman Financial Engines ($323bn AUM) confirmed a breach in January 2026. The pattern, targeting advisory firms with HNW client data, is directly applicable to UK wealth managers, IFAs and private investor platforms.

3. AI-enhanced attack capabilities

Threat actors across all categories are now generative-AI first in **Cyber Kill chain** steps 1 & 2 to enhance attack efficiency to under 60 minutes. The NCSC's 2025 Annual Review confirmed that actors linked to China, Russia, Iran and DPRK are operating large language models (LLM's) to evade detection, support reconnaissance, automate post-breach stages, and conduct AI-assisted vulnerability research and exploit development. The financial sector currently is experiencing specific AI-enhanced threats in the following areas:

- Deepfake Senior role and Partner impersonation: approximately £100 million was lost to investment scams driven by **deepfake videos** in the first half of 2025 alone (NCSC). Deloitte reports deepfake incidents increased by up to 700% in certain financial industry segments. UK Finance has specifically warned that criminals are impersonating executives to initiate fraudulent transactions, a direct threat to investment authorisation and fund transfer workflows. As Diffusion and Transformer models accelerate faster than detection capabilities, and human capabilities to accurately detect increasing more realistic deep fakes gets harder, this is an increasing exploitation gap.
- High curated, lower confidence scoring, AI-generated **spear phishing**: fully automated, highly personalised and confidence score tested phishing campaigns are now being generated at scale against financial services staff. Financial services remains the most impersonated industry for phishing at **34%** of all activity, and phishing is the initial access method in **46%** of attacks targeting the sector. Threat actors will typically analyse MX records for email security identification and confidence test highly curated emails with current topic alignment to target individuals.