BCLP. Client Intelligent

Insights

CYBER LITIGATION IN FINANCIAL SERVICES: MANAGING THE EVOLVING RISK

Jun 04, 2026

SUMMARY

Cyber incidents are increasingly giving rise to complex, long-tail litigation risk, particularly for financial services firms. As regulators place growing emphasis on operational resilience, outsourcing governance and accountability, the same regulatory findings may be repurposed to support civil follow-on claims long after incidents occur.

Regulatory investigations are taking longer to conclude and, alongside damages claims, courts are showing an increased willingness to grant urgent injunctive relief to prevent data misuse. As a result, firms should approach cyber preparedness not only as a regulatory or operational issue, but as a litigation risk mitigation exercise – aligning regulatory engagement, disclosure decisions and contractual liability planning from the outset.

This article is the second in our three-part Emerging Themes in Financial Regulation & Disputes 2026 series and follows our earlier analysis of cyber resilience and the 2026 regulatory shift. It examines the evolving litigation and regulatory landscape shaping cyber and operational resilience expectations for the year ahead and identifies practical priorities for financial services firms seeking to respond proactively. Our accompanying articles consider (i) cyber resilience and the 2026 regulatory shift; and (ii) operational resilience and the growing influence of critical third-party designations.

INCREASING LITIGATION RISK FOR FINANCIAL SERVICES FIRMS

According to ICO incident trend reporting, financial services remains one of the sectors most consistently affected by cyber-attacks. In recent years, an increasing number of corporate victims of publicised cyber incidents have faced fines from the ICO and then associated high-profile group civil claims. While those claims have encountered significant procedural and substantive hurdles – and have not yet produced the scale of damages seen in areas such as competition law litigation – their persistence underscores a continuing litigation risk for regulated firms.

© 2026 Bryan Cave Leighton Paisner LLP.

WHY FOLLOW-ON CLAIMS ARE BECOMING HARDER TO DISMISS

Although there is no current legislative proposal or formal consultation specifically aimed at facilitating group data breach claims, the broader procedural and funding landscape for collective actions continues to evolve. We have seen major developments in the consumer protection landscape with the introduction of the Digital Markets, Competition and Consumers Act 2024. And, at the time of publishing, there is an ongoing consultation published by the Law Commission on whether to introduce a collective class action regime for consumer actions. In parallel, developments in third-party litigation funding continue to reduce the practical barriers to bringing group actions.

Taken together, the drive for greater protection of consumers and their data, and the market for creating and pursuing group claims, means that while data breach claims currently remain difficult to advance, they are becoming harder for firms to dismiss entirely.

LONG-TAIL EXPOSURE IN PRACTICE – EQUIFAX AND CURRYS

Financial services firms have already experienced this risk in practice. For example, in *Atkinson v Equifax Ltd (Claim Number QB-2019-003524),* Equifax Ltd faced a civil claim following a cybersecurity breach that occurred at its parent company, Equifax Inc, which affected almost 14 million UK customers and attracted a fine of £500k from the ICO. A group claim was subsequently issued as a representative action in the High Court for breach of the Data Protection Act 1998 ("**DPA"**). That claim ultimately was withdrawn, reflecting the procedural difficulties inherent in representative actions, which require all claimants to share the "same interest".

The Currys litigation illustrates both the persistence of follow-on claims and the extended timelines that commonly characterise cyber litigation. A claim brought by 711 claimants following a 2017-2018 cyber-attack affecting Currys' point-of-sale systems was launched in August 2023. In *Sutton v Currys (Claim Number KB-2023-003287),* the claimants alleged breaches of the requirement under the DPA to take appropriate technical and organisational measures to protect personal data. The High Court stayed the proceedings pending the resolution of an appeal arising from ICO's 2020 enforcement action, reflecting an increasingly common pattern whereby civil claims are paused while regulatory challenges are resolved. Currys (DSG Retail Limited) subsequently succeeded in its appeal to the Upper Tribunal. However, the ICO then appealed that decision and was successful before the Court of Appeal in February 2026, which agreed with the First Tier Tribunal's ("**FtT**") conclusion regarding the interpretation of "personal data" and remitted the matter to the FtT for determination in accordance with its judgment. This procedural history is demonstrative of the potential extended lifespan of cyber litigation and the complexity of managing parallel regulatory and civil processes.

THE LIMITS OF GROUP DATA CLAIMS IN THE ENGLISH COURTS

© 2026 Bryan Cave Leighton Paisner LLP.

Recent cases demonstrate both ongoing claimant appetite for group litigation following data incidents and the continued limits of such claims in the English courts. In March 2026, a group data protection claim was issued against Virgin Media in relation to an alleged customer data exposure affecting a significant customer population between 2020 and 2021. This claim is particularly interesting as it relates to an incident that spanned an extended period of time and involved a substantial number of affected individuals.

Earlier litigation, including judgment from the Supreme Court on the requirement to prove, and the definition of, individual damage, highlights both the scale of potential claims and the legal barriers claimants face. For example, the claim in *Various Claimants v WM Morrison Supermarkets Plc [2020] UKSC 12*, by over 5,500 employees following the deliberate disclosure of payroll data by a rogue employee, ultimately failed and remains a landmark authority on vicarious liability in the data protection context.

These cases sit against a broader backdrop of increasing group litigation activity in the UK, although the picture is uneven rather than one of straightforward expansion. Several prominent funded claims have been withdrawn or have failed, underlining that procedural and substantive barriers remain significant. Market data nevertheless suggests a concentration of group litigation activity since 2020, accompanied by a marked increase in opt-out collective proceedings under the Competition Act 1998 since 2021. While competition and data protection claims raise distinct legal issues, these developments point to a maturing procedural and funding infrastructure that claimant firms may seek to adapt to the cyber and data breach context where factual and regulatory conditions permit.

PSEUDONYMISATION, LOSS OF CONTROL AND EVOLVING DAMAGES THEORIES

The Currys litigation is also interesting to follow for what it indicates about the limits of pseudonymisation as a risk mitigation strategy. Measures such as tokenisation or truncation of payment card data are often treated as reducing exposure. However, the case demonstrates the continuing scope for such data to be characterised as personal data where it can be linked back to an individual by the controller. For financial services firms, this reinforces the risk that reliance on pseudonymisation alone may not be sufficient to defeat data protection claims at the pleading stage, and that courts may scrutinise how such measures operate in practice rather than how they are described in policy.

A recent EU decision, while not directly binding in the UK, provides a useful comparator on the scope of remedies available following a data breach. In *IP v Quirin Privatbank C-655/23*, a job applicant sought an order preventing a bank from processing their personal data following an unlawful disclosure, rather than seeking compensation. The EU Court of Justice ("**CJEU**") clarified the scope and meaning of 'non-material damage' and held that the EU General Data Protection Act ("**EU GDPR**") does not confer a standalone right to injunctive relief restraining future data

© 2026 Bryan Cave Leighton Paisner LLP.

processing. However, the CJEU also confirmed that member states are free to provide such remedies under national law, as the EU GDPR framework is not exhaustive.

The decision forms part of an evolving body of authority on non-material damages and the concept of loss of control over personal data. While the CJEU has consistently held that loss of control does not automatically constitute compensable harm, recent cases suggest that damages may be recoverable where concrete adverse consequences can be shown. These issues are likely to be examined further by the English courts in 2026, including in Farley v Equiniti, which is due to be considered by the UK Supreme Court and is expected to address fundamental questions regarding compensation in group data breach claims.

THE PRACTICAL CONSEQUENCE – PROLONGED EXPOSURE

Dealing with cyber-related litigation, even at an early stage or for the purpose of seeking strike-out, is time-consuming and costly. Where such claims follow adverse regulatory findings, firms can face prolonged periods of uncertainty and exposure, with claims ongoing long after the underlying incident has been resolved.

OTHER ACTIONS

Even where a representative group action cannot proceed, firms may still face a range of other litigation and enforcement risks, including:

- Customer and consumer claims – Individual claims for breach of statutory duty under the UK GDPR.
- Contractual and supply-chain disputes – Business-to-business claims against technology vendors or service providers, including contractual claims based on failures to implement appropriate cybersecurity measures, and negligence claims relating to the storage or processing of customer data.
- Securities and market disclosure risk – Derivative actions by shareholders against directors under sections 260 to 264 of the Companies Act 2006. Claims under section 90 FSMA alleging that the market was misled about the adequacy of a firm's systems and controls. Although such claims remain relatively limited in number, more than 80% of section 90 FSMA claims brought in the past 12 years have been issued since 2020. In a cyber context, prolonged regulatory scrutiny following an incident may lead to historic disclosures being revisited once regulatory processes conclude.
- Regulatory civil enforcement – Civil action by the FCA under the market abuse regime where a listed firm fails to disclose inside information as soon as possible without a legitimate basis for delay, potentially resulting in fines and public censure under the Disclosure and Transparency Rules and the UK Market Abuse Regulation.

© 2026 Bryan Cave Leighton Paisner LLP.

Courts have also shown a willingness to grant urgent injunctive relief against persons unknown to prevent the dissemination or misuse of data obtained through cyber-attacks. Such relief has become an important rapid-response tool alongside regulatory and damages-based remedies and should be considered as part of incident response planning.

HYPOTHETICAL SCENARIO: HOW CYBER LITIGATION RISK CAN UNFOLD IN PRACTICE

The following scenario illustrates how cyber incidents can give rise to delayed but significant litigation exposure.

A UK-authorised financial services firm suffers a ransomware incident affecting customer data hosted by a third-party service provider. The incident is contained quickly, systems are restored and the appropriate regulators are notified. An internal review finds limited evidence of data misuse, and customer remediation measures are implemented. However, the FCA opens a supervisory investigation focusing not only on the incident itself, but on the firm's outsourcing arrangements, systems and controls, escalation processes and senior management oversight.

The investigation continues for an extended period while evidence is gathered and potential enforcement action is considered. No civil claims are brought during this period, as potential claimants await the outcome of the regulatory process. Several years later, the FCA publishes its findings, identifying weaknesses in oversight of the third-party provider and deficiencies in incident management and internal controls.

Shortly afterwards:

- individual customers bring data protection claims alleging distress and loss of control, relying heavily on the regulator's findings;
- a claimant law firm, supported by third-party funding, explores the viability of a group action; and
- the firm considers claims against its service provider, only to find that contractual liability caps and exclusions materially limit recovery.

The cyber incident itself may be historic, but the litigation and liability risk is only beginning – shaped by prolonged regulatory scrutiny and enabled by a funding environment that supports long-tail, complex claims.

WHAT THIS MEANS IN PRACTICE

PREPARING FOR PARALLEL INVESTIGATIONS AND LITIGATION

© 2026 Bryan Cave Leighton Paisner LLP.

Regulatory enforcement should be treated as an integral part of the litigation risk landscape. Explanations of systems, controls and governance provided to regulators may later be relied upon by claimants. Legal, regulatory, risk and communications teams should therefore be engaged early to ensure a consistent approach across all forums.

EVIDENCE PRESERVATION

Where investigations and claims may arise years after an incident, evidence preservation is critical. Firms should plan for early and defensible preservation of documents, communications and decision-making records, including consideration of legal privilege and how investigative material is created and retained.

SUPPLY CHAIN LIABILITY POSITIONING

Cyber litigation risk frequently centres on responsibility for third-party failings. Weak contractual positioning can leave firms absorbing losses with limited recourse. The gap between losses caused by a cyber incident and losses recoverable from suppliers should be addressed at contract negotiation stage, not after an incident occurs.

INCIDENT-RELATED DISCLOSURE OBLIGATIONS

Firms should consider how early statements, notifications and disclosures may later be challenged as incomplete or misleading, and how decisions taken under time pressure could be reframed years later through a litigation or securities claim lens.

Effective preparation requires firms to treat cyber preparedness, regulatory engagement and litigation risk as a single, integrated discipline rather than sequential responses to the same event.

CONCLUSION

Cyber incidents should no longer be treated as isolated operational or compliance events. For financial services firms, they are now best understood as litigation-enabling moments that crystallise risk across regulatory, civil, contractual and shareholder fronts – often years after the incident itself.

Firms that wait until claims emerge to consider litigation exposure will already be on the back foot. The most effective mitigation now happens before an incident occurs and in parallel with regulatory engagement, not after enforcement action has concluded.

In practice, this means senior management and boards should:

- Stress-test cyber response plans through a litigation lens, including how regulatory findings could later be pleaded in civil claims;

© 2026 Bryan Cave Leighton Paisner LLP.

- Align cyber incident governance, disclosure and communications strategies to ensure consistency across regulatory, customer and market-facing statements; and
- Identify and address contractual and outsourcing vulnerabilities that may amplify follow-on disputes following a cyber event.

As cyber regulation tightens and claimant strategies continue to evolve, the firms best placed to manage risk will be those that treat cyber resilience, regulatory compliance and litigation preparedness as a single, joined-up discipline – rather than sequential problems to be dealt with in isolation.

The authors would like to thank Siobhan La Roche–Seeley (Trainee Solicitor) for her assistance in the preparation of this article.

RELATED CAPABILITIES

- Financial Regulation Compliance & Investigations
- Litigation & Dispute Resolution

© 2026 Bryan Cave Leighton Paisner LLP.

MEET THE TEAM

Clare Reeve Curatola

Partner, London

clare.reevecuratola@bclplaw.com
+44 (0) 20 3400 3326

Caroline Cwiertnia

Associate, London

caroline.cwiertnia@bclplaw.com
+44 (0) 20 3400 2144

Samantha Paul

Knowledge & Innovation Counsel, London

samantha.paul@bclplaw.com
+44 (0) 20 3400 3194

© 2026 Bryan Cave Leighton Paisner LLP.

Anna Blest

Knowledge & Innovation Counsel,
London

anna.blest@bclplaw.com
+44 (0) 20 3400 4475

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.