# Marks & Spencer faces potential £260 million claims after major data breach



Marks & Spencer (M&S) is bracing for potential claims that could amount to hundreds of millions of pounds following a significant cyberattack that compromised customer data. The retailer has revealed that hackers infiltrated its systems over the past three weeks, gaining access to sensitive information such as contact details, dates of birth, and online order history. Importantly, M&S clarified that no payment or card details were stolen and reported no evidence of data being shared. However, the company has advised customers to remain vigilant against possible phishing attempts via emails, calls, or texts masquerading as official communications from M&S.

Legal experts are now suggesting that M&S may face numerous compensation claims, leveraging a growing trend in consumer protection. Luke Harrison, a partner at Keidan Harrison, pointed out that customers could seek compensation even in the absence of tangible financial loss. Individuals may claim damages equivalent to the "notional price" they would demand for their data's unauthorised use. He emphasised the potential for class action lawsuits to emerge, citing the efficiency of firms that utilise social media to attract claimants.

“The clients are passengers while the law firm runs the claim,” Harrison explained, indicating that law firms could negotiate settlements on behalf of their clients. This kind of litigation has precedent, as demonstrated by the case of British Airways (BA), where 16,000 claimants successfully won a class action following a major data breach in 2018—an incident that involved significant personal information and resulted in a confidential settlement in 2021. The model for claiming compensation is set to be similarly high for M&S, particularly with an active membership base of 18 million for its loyalty app.

Melanie Hart from Kingsley Napley noted that the concept of "loss of control damages" could play a pivotal role in these claims, underscoring the anxiety generated by data breaches even if participants did not suffer direct financial losses. Harrison suggested that M&S may prefer to offer voluntary compensation to evade a protracted legal battle, a common tactic employed by companies facing such allegations.

Cybersecurity experts are also on high alert regarding the fallout from this breach. Charlotte Wilson, head of enterprise at Check Point Software, has stated that the nature of the stolen data increases the risk of targeted phishing attacks. Based on historical trends, companies often observe spikes in such scams following data breaches where personal histories, including usernames, are compromised.

M&S has taken steps to mitigate further damage. In its statement, the retailer confirmed that it has reported the incident to relevant authorities, including law enforcement, in cooperation to investigate the breach thoroughly. Legal analysts, however, have raised concerns about the scrutiny M&S will face regarding its security protocols. Benjamin Ross, global head of privacy at Bortstein Legal Group, pointed out that the Information Commissioner’s Office (ICO) could impose fines if it finds M&S at fault, with potential penalties capped at 2% of the company's annual turnover, which could translate to around £260 million.

Interestingly, M&S is not alone in this predicament; shortly after its announcement, the Co-op Group also disclosed that customer data had been compromised in a separate breach. Retailers are now under increased pressure to fortify their cybersecurity measures, as data breaches not only threaten customer trust but also open the door for extensive legal repercussions. The evolving landscape of data protection laws, particularly under the UK's General Data Protection Regulation (UK GDPR), reinforces the obligation of companies to protect personal data and respond adequately to breaches.

As the legal implications of M&S’s data breach continue to unfold, affected customers and legal experts alike will be closely monitoring how the situation evolves, particularly in light of the historical context and potential for similar claims to emerge across the sector.

### Reference Map

1. Paragraphs 1, 2, 3, 4, 5, 6
2. Paragraph 2
3. Paragraph 4
4. Paragraph 5
5. Not referenced
6. Not referenced
7. Not referenced

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.thegrocer.co.uk/news/mands-could-face-class-action-compensation-claims-over-customer-data-breach-lawyers-warn/704420.article> - Please view link - unable to able to access data
2. <https://www.databreachclaims.org.uk/data-breach-compensation/marks-and-spencer-data-breach-compensation-capita> - This article discusses the potential for Marks & Spencer (M&S) to face compensation claims following a data breach involving Capita, an outsourcing group. The breach compromised personal data of various clients, potentially including M&S employees and their pension information. The article outlines the criteria for making a personal data breach claim, the roles of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) in protecting personal data, and the potential impacts of the breach on affected individuals. It also explains the concept of 'No Win No Fee' agreements and how they can benefit claimants.
3. <https://www.gordonsllp.com/uk-data-breach-compensation-claims-influenced-by-eu-court-rulings/> - This article examines how recent European Court of Justice (CJEU) rulings have influenced UK data breach compensation claims. It highlights a High Court judgment stating that claimants must demonstrate actual damage or distress resulting from a data breach to be eligible for compensation. The article discusses the case of Farley and others v Paymaster (1836) Ltd, where 400 police officers sought compensation for anxiety and distress caused by their personal data being sent to outdated addresses. The piece emphasizes the importance of showing tangible harm in data breach claims.
4. <https://www.mcglinchey.com/our-work/successfully-settled-a-putative-class-action-involving-data-breach-claims-on-a-single-plaintiff-basis/> - This article details a successful settlement of a proposed class action involving data breach claims on a single-plaintiff basis. The case highlights the complexities of data breach litigation and the challenges in achieving class certification. The article discusses the legal strategies employed, the negotiation process, and the factors that led to the settlement. It provides insights into the intricacies of data breach class actions and the importance of tailored legal approaches in such cases.
5. <https://www.xmza.com/research/markets/allNews/reuters/mondelez-law-firm-bryan-cave-reach-deal-to-end-data-breach-class-action-53939569> - This article reports on a tentative $750,000 settlement reached between Mondelez and law firm Bryan Cave Leighton Paisner to resolve a proposed class action lawsuit over a 2023 data breach. The breach compromised personal information belonging to thousands of Mondelez employees. The article details the terms of the settlement, the denial of wrongdoing by the parties involved, and the implications for data breach litigation. It provides context on the growing trend of data breach class actions and the challenges companies face in addressing such incidents.
6. <https://www.classaction.org/news/7.25-million-berry-dunn-mcneil-and-parker-settlement-ends-data-breach-lawsuit> - This article discusses a $7.25 million settlement agreed upon by Berry, Dunn, McNeil & Parker to resolve a proposed class action lawsuit alleging the firm failed to protect the personal information of approximately 1.1 million people from a data breach. The breach was discovered on September 14, 2023, and the settlement aims to compensate affected individuals. The article provides details on the nature of the breach, the settlement terms, and the broader context of data breach class actions in the United States.
7. <https://www.legalhelpline.co.uk/gdpr-data-breach-compensation/hm-gdpr-data-breach-compensation-claims/> - This article provides a comprehensive guide on H&M's GDPR data breach compensation claims, detailing how individuals can claim compensation for data breaches. It explains the types of compensation available, including material and non-material damages, and outlines the process for reporting a data breach to the Information Commissioner’s Office (ICO). The article also discusses the concept of 'No Win No Fee' agreements and how they can benefit claimants. It offers insights into the legal framework surrounding data protection and compensation in the UK.