# Hundreds of Scottish customers launch class action after Marks & Spencer cyberattack compromises data



Hundreds of Scottish customers have initiated a class action lawsuit against Marks & Spencer (M&S) following a significant cyberattack that compromised personal data and disrupted online services. This legal action, spearheaded by Thompsons Solicitors, is a response to M&S's failure to safeguard sensitive information, which may include telephone numbers, home addresses, dates of birth, and online ordering histories of millions of customers. The announcement of this lawsuit came after the Sunday Mail unveiled the breach, prompting widespread concern among affected individuals.

Following the cyber incident, M&S has paused all online and app orders, leading to empty shelves in some branches and estimated losses of up to £3.5 million per day. The attack, which occurred in April, has notably impaired M&S's online clothing sales for over three weeks, causing industry experts to estimate potential compensation claims in the UK could exceed £100 million. Patrick McGuire, a senior partner at Thompsons Solicitors, stated, “Since The Sunday Mail highlighted the launch of our class action against Marks and Spencer, we have been contacted by many more additional Scottish victims of the data theft.” He stressed the seriousness of the crime and M&S's responsibility to protect its customers.

The ramifications of this incident extend far beyond immediate financial losses; the total bill from the cyber breach is estimated at £300 million, with M&S's market value significantly impacted. The retailer’s shares have plummeted by 13% since the attack, resulting in a loss of over £750 million in market capitalisation. Despite these setbacks, in-store sales have remained stable, offering a glimmer of resilience amidst the turmoil. Nonetheless, the incident has raised vital questions regarding data security protocols and the reliance on third-party providers.

The cyberattack underscores a troubling trend of increasing cybercrime within the retail sector, heightened by the complexity of third-party contractor access to corporate systems. Evidence suggests that the hacking group Scattered Spider exploited this vulnerability, leveraging a contractor's access to penetrate M&S's IT networks. This incident has sparked wider scrutiny not only on M&S but on the broader landscape of IT security across multinational retailers, as similar attacks have been reported against companies like Co-op and Harrods.

In the wake of the attack, M&S's pledge to restore e-commerce operations by July remains uncertain. The company is currently in the process of cleaning its IT systems, involving a thorough review of more than 600 applications and thousands of servers. M&S's CEO Stuart Machin described the breach as “the most difficult challenge faced by his team,” committing to a controlled recovery. However, the incident has spurred fears about vulnerability to future scams; many newly affected customers have already reported scam attempts, further complicating the fallout from the breach.

Going forward, M&S is likely to face increasing scrutiny regarding its cyber insurance protocols. The company is set to claim up to £100 million from its insurance policies, a necessary lifeline considering the substantial lost revenues and persisting operational disruptions. Yet, as M&S navigates the aftermath of this crisis, the potential for increased insurance premiums looms large unless significant improvements are made in cyber risk management.

Ultimately, this episode not only showcases the vulnerabilities present in retail cybersecurity frameworks but also serves as a cautionary tale about the necessity of robust data protection strategies. As the digital landscape continues to evolve, companies like M&S must prioritise safeguarding customer information to prevent such breaches from recurring, ensuring that consumer trust is maintained in an increasingly digital marketplace.

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

## Bibliography

1. <https://www.dailyrecord.co.uk/news/hundreds-scots-join-class-action-35282317> - Please view link - unable to able to access data
2. <https://www.ft.com/content/c658645d-289d-49ee-bc1d-241c651516b0> - Tata Consultancy Services (TCS) is conducting an internal investigation to determine if it was the entry point for a major cyberattack on Marks and Spencer (M&S) that compromised customer data and crippled the retailer's online clothing business for over three weeks. The attack caused an estimated £300 million hit to M&S's operating profit and resulted in a market capitalization loss of over £750 million. While M&S CEO Stuart Machin attributed the breach to human error involving a third-party contractor’s staff, he did not disclose whether a ransom was paid or if TCS—which has been M&S’s primary technology partner since 2018—was directly involved. Both TCS and M&S have refrained from official comments. The UK police have launched an investigation, and TCS expects to conclude its probe by the end of the month. The incident has cast a shadow over TCS’s reputation amidst a broader increase in cybercrime affecting UK retailers and India's tech industry. TCS, also partnered with UK retailer Co-op, confirmed its services were not linked to a separate cyberattack on that company. The event highlights growing cybersecurity challenges faced by global IT service providers.
3. <https://www.reuters.com/business/media-telecom/britains-ms-says-cyberattack-cost-400-million-2025-05-21/> - Marks & Spencer (M&S), a major British retailer, announced that a sophisticated cyberattack will reduce its operating profit by approximately £300 million ($403 million), with disruptions expected to persist into July. The attack temporarily shut down M&S's online clothing operations, disrupted food supplies, and wiped over £1 billion from its market value. Although online sales in the fashion, home, and beauty sectors were heavily impacted, in-store sales remained stable. The food division experienced reduced availability and higher logistics costs due to reverting to manual operations but has since shown signs of recovery. M&S aims to mitigate half of the profit loss in the 2025/26 fiscal year through insurance and cost management. Shares in the retailer fell by 13% since the incident. Despite the setback, the company remains committed to accelerating its technology transformation and recovery efforts. CEO Stuart Machin emphasized resilience and customer support. The incident follows an increasing trend of cyberattacks targeting UK businesses, which have also affected Co-op, Harrods, and the British Library. Meanwhile, M&S reported strong financial results prior to the attack, including a 22.2% rise in adjusted pretax profit and a 6.1% sales increase, benefitting food and clothing segments. Competitors like Next, Tesco, and Sainsbury’s may gain from M&S's online setbacks.
4. <https://www.ft.com/content/19dcd993-877e-43c5-aab4-c727e574e3f2> - Marks & Spencer (M&S) faced a significant cyber attack that compromised its operations and is expected to cut up to £300 million from this year’s operating profit. The attack forced the shutdown of its online clothing business for over three weeks, resulting in stolen customer data and a £750 million market capitalisation loss. The breach occurred due to social engineering tactics directed at a third-party supplier, allowing cybercriminals to bypass M&S’s internal defenses. Although M&S had significantly increased its investment in cybersecurity and expanded its security team, the incident exposed its vulnerability through third-party dependencies—a common risk for multinational retailers. In response, M&S is undertaking a comprehensive cleansing of more than 600 applications and thousands of servers, with full e-commerce operations expected to resume by July. CEO Stuart Machin described the attack as the most difficult challenge faced by his team, and the company is now focusing on a controlled and thorough recovery to ensure long-term security. The incident has also raised questions about potential cuts to executive bonuses and has heightened scrutiny of third-party IT partnerships in the retail industry.
5. <https://www.ft.com/content/723b6195-1ce7-4b5f-94f5-729e9152c578> - Marks and Spencer (M&S) stands to claim up to £100 million from its cyber insurance following a recent cyberattack, which compromised some customer data and severely disrupted operations, especially online orders for almost three weeks. The personal data exposed includes contact details, dates of birth, and order histories, though not payment details or passwords. Insurers involved include Allianz, expected to cover at least £10 million initially, and Beazley. The incident may have resulted in lost revenues exceeding £60 million and contributed to a 16% drop in share price, erasing £1.3 billion of its market value. M&S's cyber insurance, arranged by WTW, is likely to cover all losses, including both direct and third-party liabilities, even if a third-party vendor is implicated in the breach. However, M&S may see its insurance premium—currently under £5 million—double unless it improves cyber risk management. This breach, along with recent cyberattacks on other UK retailers such as Harrods and the Co-op, may lead to increased cyber insurance premiums across the sector. The M&S payout could validate the value of cyber insurance and encourage wider adoption among smaller businesses. UK businesses have suffered approximately £44 billion in cyber-related revenue losses over the past five years.
6. <https://www.bbc.com/news/technology-34656818> - Marks and Spencer's website experienced a fault that allowed customers to view each other's personal details upon logging into their own accounts. The retailer temporarily suspended its site for two hours to fix the problem, attributing the glitch to an internal error rather than an external hack. The exposed information included names, dates of birth, contact details, and previous orders. M&S apologized for the incident and assured customers that no full credit card details were among the exposed information. The company emphasized that personal information such as account details was kept in a completely separate place.
7. <https://www.bbc.com/news/technology-12983177> - Marks and Spencer customers were warned to expect an increase in spam emails after hackers stole their details from marketing firm Epsilon. The company contacted users of its online service to inform them about the data breach, which was part of a wider attack on Epsilon. M&S assured customers that no other personal information, such as account details, had been accessed or was at risk. Epsilon admitted to an unauthorized entry into their systems and clarified that the breach affected 2% of total clients, including many big banks and retailers. A full investigation was underway.