# Marks & Spencer faces multimillion-pound class action after prolonged cyberattack disruption



Marks & Spencer (M&S) is embroiled in a significant legal battle, facing a multimillion-pound class action lawsuit following a severe cyberattack that compromised customer data. This incident, which has devastated the retailer's online operations for nearly a month, has raised concerns over data security and consumer protection. The company confirmed that hackers accessed customer information including contact details, dates of birth, and online order histories, though no payment or password data were stolen. Despite these reassurances, the possibility exists that affected customers may fall prey to phishing scams, leading M&S to issue cautionary advisories.

Thompsons Solicitors, a Scottish law firm, is spearheading the class action against M&S, claiming that the retailer's failure to adequately safeguard customer data has exposed its clients to potential fraud. Senior partner Patrick McGuire indicated a surge in client inquiries from concerned M&S customers, asserting that this could be one of the largest data theft cases in the firm’s history. "Group litigation means that the public can hold M&S to account for the theft of their details,” he stated, emphasising the importance of consumer rights in the face of corporate negligence.

The legal perspective on this breach is multifaceted, as articulated by legal experts who suggest that customers could seek compensation based on the "loss of control damages," reflecting the anxiety that accompanies such data breaches. Luke Harrison, a partner at Keidan Harrison, explained that claims, albeit potentially modest at around £500 each, could accumulate substantially, especially with an extensive customer base.

In addition to facing legal ramifications, M&S has experienced severe operational setbacks. The cyberattack, attributed to the ransomware group Scattered Spider and DragonForce, has reportedly cost the company over £60 million in lost profits, with more than £1 billion shaved off its market valuation. The disruption has halted online orders, which typically account for a third of M&S's clothing and home revenue, sparking concerns that prolonged outages could alienate customer loyalty.

Despite the chaos, the retailer has opted not to pay any ransom, in line with UK government recommendations, choosing instead to concentrate on fortifying its cybersecurity measures. Analysts have raised alarm that these decisions, while strategically sound, may prolong the recovery process and lead to lasting reputational damage. It remains critical for M&S to resume online operations swiftly, as customer experience is now intricately tied to confidence in the retailer's cybersecurity resilience.

Financial analysts have predicted a challenging road ahead for M&S, particularly as it prepares for its annual results announcement. While the retailer generated a strong financial performance prior to the breach, the repercussions of this incident are anticipated to bleed into its future earnings. CEO Stuart Machin could personally feel the impact too, facing significant financial losses linked to the attack, which has contributed to a pronounced drop in share price.

Interestingly, M&S might recover some losses through its cyber insurance, claiming up to £100 million. However, the potential for increased premiums looms over the company if cybersecurity measures do not improve significantly. As the current retail landscape faces heightened cyber threats, M&S's experience serves as a sobering reminder for other retailers to bolster their defenses against the ever-evolving cyber threat landscape.

As the situation develops, the key questions remain: how effectively will M&S navigate this crisis, and what lessons will the broader retail sector glean from this major incident? The outcome could reshape not only M&S’s operational strategies but also the standards for cybersecurity across the industry.

### Reference Map

1. Paragraph 1, 2, 3, 4, 5.
2. Paragraph 6.
3. Paragraph 7.
4. Paragraph 8.
5. Paragraph 9.
6. Paragraph 10.

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

## Bibliography

1. <https://www.thegrocer.co.uk/news/cyberattack-mands-facing-class-lawsuit-over-customer-data-theft/704629.article> - Please view link - unable to able to access data
2. <https://www.reuters.com/business/retail-consumer/ms-slow-recovery-cyberattack-puts-it-risk-lasting-damage-2025-05-19/> - A month after a cyberattack crippled Marks & Spencer's (M&S) online operations, the UK retailer is still struggling to fully recover, prioritizing cybersecurity over rapid system restoration. The attack, attributed to the ransomware group Scattered Spider and DragonForce, has already cost M&S an estimated £60 million in lost profits and over £1 billion in market value. Online clothing and home orders remain suspended, and some in-store products have also been affected due to disrupted supply operations. The company is gradually bringing systems back online and has resumed food stock forecasting. M&S refused to pay the ransom in line with government guidance, opting to rebuild its systems, a move that may prolong disruptions and potentially lead to reputational harm. Analysts warn continued delays risk customer frustration, rising operational costs, and reduced morale among staff. The breach reportedly involved credentials of Tata Consulting Services employees, though TCS has not commented. With online sales typically comprising a third of M&S’s clothing and home revenue, the disruption could result in substantial losses. Meanwhile, other UK retailers are urgently reassessing cybersecurity to avoid a similar fate, acknowledging the widespread vulnerability in the retail sector.
3. <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.
4. <https://www.ft.com/content/43531d25-4f7a-4d6e-b809-e85bb8f0033e> - Marks and Spencer (M&S) CEO Stuart Machin is set to lose up to £1.06 million from his pay package due to a cyber attack that triggered a 14% drop in the company’s share price. Machin, appointed in 2022, stands to lose £831,000 from a performance share plan and £233,000 from a deferred bonus vesting in July, with total potential losses reaching around £2.4 million when considering his remaining incentive shares. The cyber attack, disclosed in April 2025, compromised customer data, disrupted online orders for three weeks, and led to stock shortages in stores. Analysts estimate the retailer may have already lost around £75 million in revenue, with potential losses rising to £125 million if disruptions continue through May. While M&S may claim up to £100 million in insurance, the incident risks affecting its broader transformation efforts, including back-end automation and digital improvements. Despite the setback, M&S posted a strong financial year prior to the attack, with expected pre-tax profits of £840 million and a 14.7% year-on-year sales increase. However, the damage from the cyber incident may weigh heavily on first-quarter 2026 performance and long-term strategy execution.
5. <https://www.reuters.com/business/retail-consumer/uks-ms-says-food-availability-improving-every-day-2025-05-15/> - British retailer Marks & Spencer (M&S) announced that food supplies from its distribution centers to stores have returned to normal levels following a cyberattack that disrupted operations last month. The company reported that, particularly in chilled food sections, customer needs are being met, and deliveries to grocery departments are stabilizing, leading to daily improvements in product availability. The cyberattack, first acknowledged on April 22, led to the temporary shutdown of systems, affecting stock availability across food, clothing, and home departments. Additionally, M&S revealed that some personal customer information was compromised during the breach. Online clothing orders remain suspended since April 25, with no current update on when they will resume.
6. <https://www.reuters.com/business/retail-consumer/uks-ms-says-customer-information-was-taken-cyber-attack-2025-05-13/> - British retailer Marks and Spencer (M&S) confirmed it suffered a cyber attack that compromised some customer personal data, though no usable payment information or passwords were taken. The attack, widely identified as a ransomware incident, has significantly disrupted M&S's online operations, halting online orders since April 25. Despite the breach, M&S emphasized there is no evidence the stolen data has been shared and reassured customers that no action is required from them at this time. The company is working with cybersecurity experts, law enforcement, and government agencies to restore operations and secure its systems. While its 1,000 physical stores remain operational, M&S has seen a 15% drop in share price and is facing substantial financial impact, particularly as online sales represent about a third of its clothing and home revenue. Deutsche Bank analysts estimate the profit loss could be at least £30 million, with weekly losses around £15 million. M&S noted that cyber insurance may cover most of the damages, though typically for a limited period.
7. <https://moneyweek.com/personal-finance/marks-and-spencer-online-order-problems> - Marks & Spencer (M&S) continues to face serious operational disruptions following a cyberattack that occurred over the Easter weekend. Online orders through its website, app, and phone have been suspended since April 25, with no confirmed restart date. The attack compromised some customer data, including names, contact information, and order histories, though no payment details or passwords were exposed. As a security measure, customers will be prompted to reset their passwords upon their next login. Services including Sparks loyalty offers have been paused, and in-store stock availability remains inconsistent, as illustrated by images of empty shelves shared by shoppers online. The cyberattack has severely impacted M&S financially, with an estimated £4 million a day in lost online sales and an 18% drop in share value, erasing over £1 billion in market capitalization. While some affected customers have been compensated with gift cards, broader investor confidence is shaken due to limited communication from M&S. The ransomware group “DragonForce” has claimed responsibility for the breach. Despite these challenges, M&S's core food business and partnerships like Ocado remain unaffected, providing a silver lining during this crisis. The company is actively working to resolve the issue though no timeline has been confirmed.