# Marks and Spencer faces class action and heavy losses after Scattered Spider cyber attack



Marks and Spencer (M&S) is currently facing significant backlash following a devastating cyber attack that has compromised the personal data of countless customers. The incident, which unfolded in late April, has prompted Thompsons Solicitors, a leading law firm, to initiate a class action suit against the retailer. This legal action seeks to hold M&S accountable for potential negligence in safeguarding customer information, which includes phone numbers, home addresses, dates of birth, and online order histories.

The ramifications of the breach are substantial. According to reports, the hackers, identified as part of a group called Scattered Spider, gained entry through a contractor to M&S’s advanced IT systems. This breach not only exposed personal data but has also led to operational disruptions, crippling M&S's online ordering capabilities for weeks. Since the attack, M&S has reportedly lost up to £3.5 million a day and witnessed a staggering £1.2 billion reduction in market value, with its share price plummeting by approximately 14%. Clive Black, a retail analyst, underlines the severity of the incident, predicting detrimental impacts on the company's performance for the coming quarters.

Patrick McGuire, Senior Partner at Thompsons Solicitors, has been vocal about the implications of this breach. He stated, “We have a situation here where one of the most famous retailers in the UK has allowed criminals to pillage the personal details of hundreds of thousands of Scottish customers,” highlighting the retailer's failure to meet its legal obligations in protecting customer data. McGuire added that this situation represents the largest case of data theft the firm has ever encountered.

M&S has been quick to reassure customers regarding the nature of the data breached, emphasising that no usable payment or card details were compromised. However, the exposure of personal information leaves customers vulnerable to identity theft and subsequent criminal scams. The retailer has urged affected customers to reset their passwords as a precautionary measure. This prompt comes amidst warnings of possible phishing attempts as cybercriminals may exploit the chaos surrounding the breach to launch targeted scams.

The implications extend beyond immediate customer concerns; the incident could also disrupt M&S’s long-term strategic plans, especially those centred on digital transformation and back-end automation. Industry experts predict that failure to rebuild its reputation could lead to lasting consequences for the retailer, particularly as they navigate the intensified competition within the sector. M&S's prior financial performance had been promising, with pre-tax profits of £840 million expected for the past year. However, the current crisis threatens to overshadow these achievements.

Cybersecurity has been a growing concern across the UK retail sector, particularly as incidents involving major companies have become more frequent. The National Cyber Security Centre has called for businesses to implement stricter security measures following these attacks, advocating for a more proactive approach to safeguard customer data. This call to action underscores a larger trend; UK businesses have incurred approximately £44 billion in losses linked to cyber-related issues over the last five years.

As M&S grapples with both the legal ramifications of the data breach and the operational challenges posed by the attack, it has also had to confront the public relations fallout. Insiders suggest that while the retailer may claim up to £100 million from cyber insurance, its insurance premiums could rise dramatically unless it evidently improves its cybersecurity protocols. The lessons learned from this incident may not only affect M&S but could also serve as cautionary tales for other retailers venturing into the complex digital landscape.

In a tumultuous time for M&S, the path to recovery is fraught with challenges. As it navigates through legal battles and strives to restore customer trust, the company must also fortify its digital infrastructure to prevent similar incidents in the future. How M&S addresses these pressing concerns will likely shape its reputation and operational viability in the competitive retail environment for years to come.

### Reference Map

1. Paragraphs 1, 2, 3, 4, 5, 6, 7
2. Paragraph 5
3. Paragraph 4
4. Paragraph 3
5. Paragraph 2
6. Paragraph 5
7. Paragraph 6

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

## Bibliography

1. <https://www.dailyrecord.co.uk/news/scottish-news/ms-face-multi-million-pound-35243849> - Please view link - unable to able to access data
2. <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. 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.
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://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.
5. <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.
6. <https://www.reuters.com/business/retail-consumer/ms-co-op-cyberattackers-duped-it-help-desks-into-resetting-passwords-says-report-2025-05-06/> - Cyberattacks on UK retailers Marks & Spencer (M&S) and the Co-op Group were initiated by hackers impersonating employees and deceiving IT help desks into resetting passwords, according to BleepingComputer. This allowed the intruders access to internal networks. The UK's National Cyber Security Centre has advised organizations to revise their help desk protocols to prevent similar breaches. M&S, having disclosed the cyber incident on April 22, witnessed a 12% share decline and subsequently suspended online clothing and home orders; food product availability has also been disrupted. Analysts from Deutsche Bank estimate the financial impact at approximately £30 million ($40 million), with ongoing losses of around £15 million weekly, though cyber insurance is anticipated to cover most of the initial losses. Full recovery may take weeks, as rebuilding networks is a complex process. Meanwhile, a group named DragonForce claimed responsibility for attacks on M&S, the Co-op, and Harrods, alleging theft of staff and potentially 20 million customer records. The attack on M&S has also been tentatively linked to the hacking group "Scattered Spider" using DragonForce ransomware, though the National Cyber Security Centre has not confirmed any direct connection between these incidents.
7. <https://apnews.com/article/7d3c01faa7380775598a517df4db1250> - British retailers are facing a wave of cyberattacks, with Marks & Spencer (M&S) and Harrods among the latest high-profile victims. M&S has been grappling with an ongoing cyber incident since Easter weekend, disabling its ability to process online orders, hire new staff, or maintain regular website functions. Although some services like contactless payments have been restored, the disruption continues as M&S works intensively to resolve the issue. Meanwhile, Harrods acknowledged a cyber threat and has taken precautionary steps, including limiting internet access. The attacks, which may be linked to a group called Scattered Spider, have raised concerns in the UK retail sector following a similar incident at Co-op. Authorities, including London’s Metropolitan Police and the UK’s National Cyber Security Centre, are investigating and providing support. Experts across the cyber defense industry warn that the growing use of generative artificial intelligence is intensifying the cyber threat landscape and urge organizations to strengthen their digital defenses.