DFI RETAIL GROUP

Cybersecurity Notice

28 September 2026 – We recently experienced a cybersecurity incident in which a financially motivated threat actor gained unauthorised access to part of our technology environment.

Based on the findings of our investigation to date, a certain amount of data was compromised. As soon as we became aware, we activated our incident response plan and engaged independent forensic and cybersecurity experts to investigate, contain the incident and help us strengthen our defences. Our teams have worked around the clock to respond to this incident and secure the affected infrastructure. Although the incident caused minimal disruptions to operations for a very short duration, the affected environment has been secured and our stores and services are now operating as normal. Throughout this process, our focus has been on protecting our customers, our people and our partners, and responding to the incident with diligence, integrity and transparency.

Our investigation is at an early stage, and what we know so far suggests that some internal documents may have been affected. We are notifying the relevant regulatory authorities and are keeping them informed as our investigation progresses, and we will comply with our regulatory obligations as facts are confirmed.

Cybercrime affects organisations and individuals across every sector. That does not lessen our responsibility to those who place their trust in us, and we do not take that trust lightly. We do not support criminal activity, and we will work with our teams and independent experts to respond to threats of this kind in the way that best protects our customers, people and business partners.

We are committed to handling this matter responsibly and in accordance with our legal and regulatory obligations. We will continue to take appropriate steps to strengthen our cybersecurity controls and safeguard our systems and data.

*****