Significant changes in shareholdings of directors and major shareholders in 2024 up to the publication date in 2025:

TFN Union Investment Co., Ltd., the major shareholder of TWM, was merged into Taiwan Fixed Network Co., Ltd. on November 1, 2024, which resulted in the transfer of 11.03% of the company's shares to Taiwan Fixed Network Co., Ltd. Since both companies are subsidiaries of TWM, this share transfer did not have any impact on the Company.

Changes in management controls in 2024 up to the publication date in 2025:

None.

Significant lawsuits and non-litigious matters in 2024 up to the publication date in 2025

1. The Company:

(1) Spectrum dispute between Far EasTone Telecommunications Co., Ltd. ("FET") and Taiwan Mobile ("the Company")

Parties Involved: FET is the plaintiff, and the Company is the defendant.

In August 2015, FET filed a civil complaint with the Taipei District Court ("District Court") demanding that the Company: (i) file an application to return the C4 spectrum block; (ii) stop using the C4 spectrum block; (iii) stop using the C1 spectrum block until its application for the return of the C4 spectrum block is approved by the NCC; and (iv) pay NT$1,005.800 million to FET as compensation.

In May 2016, the District Court ruled in favor of FET on claims (i), (ii) and (iii), and against FET on claim (iv). TWM and FET appealed these decisions to the High Court. The High Court dismissed TWM's appeal on claims (i), (ii) and (iii), and modified the judgment on claim (iv), ordering TWM to pay FET NT$765.779 million, as well as a 5% annual interest on NT$152.584 million of the aforementioned amount from September 5, 2015, until the payment date. TWM and FET appealed the rulings.

In May 2019, the Supreme Court dismissed the High Court's ruling in regard to FET's additional appeals, eliminated TWM's payment obligation, and remanded the case to the High Court. During the first retrial, TWM filed a counterclaim demanding FET pay NT$14.482 million, plus a 5% annual interest from the day after the counterclaim is served until the settlement date. In August 2020, the High Court ruled as follows: for the dismissed claim (iv), TWM must pay FET NT$242.154 million, plus a 5% annual interest on NT$142.685 million of the aforementioned amount from September 30, 2016, to the payment date, and a 5% annual interest on NT$99.469 million from July 21, 2017, to the payment date. The Company's counterclaim was denied. The Company and FET appealed the rulings. In June 2023, the Supreme Court dismissed the first retrial of the High Court and remanded the case to the High Court. The case is now in process at the second retrial of the High Court. In December 2024, the second retrial of the High Court ruled as follows: for the FET's claim (iv), TWM must pay FET NT$720.916 million, plus a 5% annual interest from September 5, 2015, to the payment date. The Company's counterclaim was denied. The Company and FET have respectively appealed the rulings. The case is now in process at the Supreme Court.

2. The Company's directors, general manager, executives, major shareholders hold more than 10 percent of the Company's shares:

None.

3. The Company's subsidiaries:

None.

Other major risks and countermeasures

In terms of information security and privacy protection, the telecommunications industry has a huge trove of personal data. If they are accidentally leaked, the Company could be held legally responsible, which could seriously damage its reputation.

Countermeasures:

TWM has implemented the ISO/IEC 27001 – Information Security Management System (ISMS) and the BS 10012, ISO/IEC 27701, 29100 – Personal Information Management System (PIMS). The Company's Cyber Security and Data Privacy Protection Committee reviews security and personal information protection policies on a quarterly basis and reports the results of ISMS and PIMS to the Board of Directors. The Company has also purchased cybersecurity insurance for advanced customer data protection. Furthermore, to ensure a four-dimensional protection of users' personal data and internal confidential data, the Company has implemented the following:

1. **Stopping external hackers:** Intrusion prevention, network segmentation, firewalls, web application firewalls, etc.
2. **Preventing internal leaks:** Conduct data leakage protection detection and strengthen gap reinforcement measures.
3. **System planning and development:** Incorporate system development security specifications and execute code scanning, etc.
4. **Operation and maintenance monitoring:** Establish an information security monitoring center, check and analyze system records, and report and track if abnormal conditions are found.

Other significant items:

None