



News Release

Singtel addresses data breach, moves to support affected stakeholders

Singapore, 17 February 2021 – Singtel has completed initial investigations into a recent breach on a third-party file sharing system and has begun reaching out to affected stakeholders.

Based on investigations and analysis conducted so far with the help of cyber security experts, the company has established which files on the Accellion FTA system were accessed illegally during the breach and which stakeholders have been impacted.

The data taken includes consumer information containing varying combinations of personally identifiable information. 23 enterprises have also been impacted. These include suppliers, partners and corporate customers. A large part of the leaked data includes Singtel's internal information that is non-sensitive such as data logs, test data, reports and emails. Singtel has begun notifying all affected individuals and enterprises to help them and their staff manage the possible risks involved and take appropriate follow-up action.

"While this data theft was committed by unknown parties, I'm very sorry this has happened to our customers and apologise unreservedly to everyone impacted. Data privacy is paramount, we have disappointed our stakeholders and not met the standards we have set for ourselves," said Singtel's Group CEO Mr Yuen Kuan Moon. "Given the complexity and sensitivity of our investigations, we are being as transparent as possible and providing information that is accurate to the best of our knowledge. We are doing our level best to keep our customers supported in mitigating the potential risks."

Mr Yuen added, "I'd like to thank our customers and partners for their patience and understanding as we continue our cyber and criminal investigations to understand the full extent of this breach. I want to emphasise that our core operations and functions remain unaffected and sound and this incident involves a standalone system provided by a third-party vendor. Information security remains our highest priority and you have my commitment that we are conducting a thorough review of our systems and processes to strengthen them."

Exfiltrated data established to date:
Personally Identifiable Information of approximately 129,000 customers containing NRIC and some combination of the following information: name, date of birth, mobile number, address
Bank account details of 28 former Singtel employees
Credit card details of 45 staff of a corporate customer with Singtel mobile lines
Some information from 23 enterprises

Singtel is moving with urgency to reach out to all affected individual and corporate customers to keep them supported on how best to manage the variable risks involved. We are also appointing a global data and information service provider, to provide identity monitoring services at no cost to affected customers to help them manage potential risks. This service monitors public websites and non-public places on the internet, and notifies users of any unusual activity related to their personal information.



As we progressively contact impacted customers, those concerned can refer to singtel.com/accellion-incident for more information.

Accellion FTA which Singtel used as a third-party file sharing system was the target of a sophisticated cyber attack exploiting a previously unknown vulnerability. When first alerted to exploits against the system last December, Singtel promptly applied a series of patches provided by Accellion to plug the vulnerability, the last patch being 27 December. On 23 January this year, Accellion advised that a new vulnerability had emerged that rendered patches previously applied in December ineffective. Singtel immediately took the system offline. On 30 January, Singtel's attempt to patch the new vulnerability in the FTA system triggered an anomaly alert. Accellion informed thereafter that the system could have been breached. Singtel's investigations later confirmed this and identified 20 January as the date the breach occurred. The FTA system has been kept offline since 23 January. On 9 February, Singtel established that files were taken as a result of the breach and informed the public two days later on 11 February.

Please refer to:

- Singtel's 11 February [media statement](#) on the Accellion security incident.
- [FAQs](#) for guidance on action that affected customers can take and other updates.

###



About Singtel

Singtel is Asia's leading communications technology group, providing a portfolio of services from next-generation communication, technology services to infotainment to both consumers and businesses. For consumers, Singtel delivers a complete and integrated suite of services, including mobile, broadband and TV. For businesses, Singtel offers a complementary array of workforce mobility solutions, data hosting, cloud, network infrastructure, analytics and cyber-security capabilities. The Group has presence in Asia, Australia and Africa and reaches over 700 million mobile customers in 21 countries. Its infrastructure and technology services for businesses span 21 countries, with more than 428 direct points of presence in 362 cities. For more information, visit www.singtel.com.

Follow us on Twitter at twitter.com/SingtelNews.

Media Contact

Lian Pek
Vice President, Group Strategic Communications and Brand
Phone: +65 94882696
Email: lianpek@singtel.com