ACME FINANCIAL SERVICES

Powered by GLESEC

CYBERSECURITY NEWS CUSTOM REPORT

Generated on 03/07/2025 by

ACCC says bank screen scraping warnings are not anti-competitive

08/10/2020 12:35

The Australian Competition and Consumer Commission (ACCC) has said warnings to consumers from banks over the use of screen scraping are not designed to lower competition in the local market, and are general security warnings.

Responding to the Questions on Notice from the Select Committee on Financial Technology and Regulatory Technology, the consumer watchdog said it had received complaints from two financial institutions on March 2 that framed the warnings as anti-competitive.

"The complaints express concern that by warning customers of these dangers, the major banks may have discouraged customers from engaging with third party neobanks or other financial service providers," the ACCC said.

"The ACCC considered the detail of the complaints and the terms of the warnings by the major banks and decided not to commence an investigation. The alleged conduct involves general statements or warnings regarding potential security or safety risks associated with screen scraping and sharing passwords, and does not appear to have the purpose or effect of substantially lessening competition."

The commission added it currently has six investigations looking into anti-competitive conduct in the finance sector, as well as working on a market study, and introducing the Consumer Data Right.

See also: Australia's Consumer Data Right: Here's everything you need to know

"All of this work is intended to enhance competition in the sector for the benefit of consumers including supporting and improving the capacity of new entrants and smaller businesses to compete in the financial services sector," the ACCC said.

The committee heard split opinions in January on whether a prohibition on screen scraping -- where customers hand over login information to a third-party to allow them to capture data directly from a web page -- is needed.

"Screen scraping is bad technology. It's just aided bad technology. It's a way around barriers that exist, but it's not actually trying to solve the underlying problem, which is helping people communicate and do what they want with their finances, pay the way they want," head of corporate development at Melbourne-based fintech startup Airwallex Dave Stein said at the time.

"We don't do that, we don't use that, but for us, it's a technology decision. We just don't want to invest in a dated technology."

Raiz Invest general counsel Astrid Raetze argued that screen scraping will always have two camps.

"There's the banks and their views, and then there are fintechs who are not bank affiliated. Largely, the argument centres around the banks saying, 'it's bad, it's wrong you have to shut it down', and then there's the fintechs who say, 'we need it'," she said.

"If you switch on open banking and turn off screen scraping … what you will do is hamstring the fintech industry."

In March, the Committee shifted focus to the aftermath of the coronavirus pandemic.

Responding last month, the Australian Medical Association said e-prescriptions and telehealth should become lasting features of Australia's health system, even once COVID-19 restrictions are eased.

"While the benefits of telehealth extend beyond mere cost savings, the permanent adoption of telehealth will reduce costs across the health system while improving patient outcomes," the AMA said.

"Telehealth can also reduce the cost of providing health care when considering the costs associated with health professionals needing to travel for home visits, and the cost to the government for rural aeromedical evacuation and health care in institutions like correctional facilities."

FBI Releases PIN on Attacks Using Significant Financial Events for Extortion

11/03/2021 12:15

The Federal Bureau of Investigation (FBI) has released a Private Industry Notification (PIN) on ransomware actors using significant financial events, such as mergers and acquisitions, to target and leverage victim companies.

CISA encourages users and administrators to review Ransomware Actors Use Significant Financial Events and Stock Valuation to Facilitate Targeting and Extortion of Victims and apply the recommended mitigations.