Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/about/contacts

PUBLIC STATEMENT

Card-Number Protections Depend on Data Deletion

Embargoed to Tuesday 2 November 2022

The Optus, Medibank and MedLab data breaches have caused some re-thinking.

But not all of the thinking is clear enough.

It's being touted that there's a simple solution to driver licence data being compromised.

That solution is said to be the addition of a card-number.

So, instead of just the licence-number and expiry-date being used to authenticate a claim that a person is entitled to use that identity document, the card-number would also be required.

This was implemented recently in NSW, and it has now been announced for immediate implementation in Victoria, with about 1m of that State's 5m licences to be urgently re-issued.

But will that achieve the aim?

Credit-cards have had a 3- or 4-digit 'card verification code' or 'card security code' on the back (variously called a CVV, CVC or CSC) since about 2000. Its function is identical to that of a card-number on a driver's licence (on the front of the card in NSW and on the back in Victoria).

The MedLab attack gained access to credit-card details – including in some cases the CVV. So the CVV was no protection against fraud, because it was accessed as part of the same attack.

If the next hacker gets the driver's licence card-number, along with licence-number and expiry-date, the card-number provides no protection at all.

Organisations have to understand that the critical issue is:

The retention of authentication-data in databases creates an unmanageable vulnerability

For vulnerability to attacks to be reduced, security-sensitive data must either:

- not be stored at all – an application of the vital principle of data minimisation; or
- be retained only for the few seconds to a minute needed for the authentication process to be completed. Then that data must be expunged, to prevent access by future hackers.

APF Source

APF Policy Statement on Information Security (December 2012)
https://privacy.org.au/policies/info-security/

0414 731 249 – David.Vaile@privacy.org.au 02 6288 6916 – Roger.Clarke@privacy.org.au

Background Information

Outline of the Three Data Breach Cases

On 22 September, telecommunications company Optus was reported as having had vast volumes of personal data extracted from its databases by persons unknown. It progressively became clear that this included **data about documents used to authenticate customers' identities, including driver's licences, Medicare cards and passport data**.

On 20 October, private health insurer Medibank was reported as having been attacked. By 25 October, it was clear that the data breach included details about where customers received medical services, the **codes relating to patients' diagnoses, and procedures**.

On 28 October, the media reported a data breach at a pathology laboratory company called MedLab, which resulted in the escape of **credit-card details sufficient to enable identity fraud, in some cases even including the security code (CVV)**. The retention of this data is in breach of industry standards, but Visa and MasterCard are not in a strong position to enforce the standards. That's the responsibility of regulatory agencies.

Relevant Media Reports

McElroy N. (2022) **'Optus** says it has been hit by a cyber attack that has compromised customer information' ABC News, 22 Sep 2022, at https://www.abc.net.au/news/2022-09-22/optus-hit-with-cyber-attack-impacting-customers-/101466036

Bonyhady N. (2022) 'How **Optus** was hacked by someone acting like a 'kid in a garage' The Sydney Morning Herald, 1 October 2022, at https://www.smh.com.au/technology/how-optus-was-hacked-by-someone-acting-like-a-kid-in-a-garage-20220929-p5bm1r.html

Bogle A. (2022) **'Past Optus customers have had their data exposed — why did the company still have it?**' ABC Science, 2 Oct 2022, at https://www.abc.net.au/news/science/2022-10-02/why-is-optus-keeping-customer-data-for-so-long/101491200

Power J. (2022) 'Confusion, chaos and concern after **Optus** text blitz' The Sydney Morning Herald, 3 October 2022, at https://www.smh.com.au/national/nsw/confusion-chaos-and-concern-in-the-wake-of-optus-text-blitz-20221003-p5bmso.html

Cowie T. (2022) 'VicRoads to issue almost 1 million free driver's licences after **Optus** hack' The Age, 29 October 29, at https://www.theage.com.au/national/victoria/vicroads-to-issue-almost-1-million-free-driver-licences-after-optus-hack-20221029-p5bu08.html

Winter V. (2022) 'All **Medibank** customers' personal data was compromised in the cyber attack' ABC News, 25 October 2022, at https://www.abc.net.au/news/2022-10-25/medibank-breach-ahm-osch-cyber-attack-data-what-to-do/101574200

Chirgwin R. (2022) '**Medlab Pathology** discloses February data breach' itNews, 27 Oct 2022, at https://www.itnews.com.au/news/medlab-pathology-discloses-february-data-breach-587030