18 February 2019 – LandMark White Limited (ASX:LMW)

Update on Data Incident

On 5 February 2019, LandMark White Limited ("LMW" or "Company") announced ("Announcement") to the market it had been the victim of a cyber security incident ("Incident") that resulted in a dataset being disclosed on the dark web. In line with the Announcement, the Company has made contact with the relevant corporate partners affected by Incident.

As of Wednesday, 13 February 2019 several of the Company's corporate partners, primarily from LMW's banking and finance panel lenders, suspended the flow of valuation instructions to LMW pending additional information from the Company in relation to the Incident. Due to this occurring, the Company requested a trading halt prior to the market opening on Thursday 14 February 2019.

During this time LMW has been working with independent cyber security consultants, along with the Australian Cyber Security Centre and the Office of the Australian Information Commissioner, to ensure client information and LMW's network is secure.

Having assessed the severity of the incident and confirming that the personal information disclosed is relatively benign, the breach was isolated and has been closed. LMW continues to work with the affected corporate partners to lift suspensions, recover work flows and return to business as usual. LMW has not obtained any evidence that the data has been misused.

We anticipate that the suspensions will be progressively lifted over the coming days and that workflows will return to more normal levels by the end of the month.

The dataset disclosed was limited to property valuation and some personal contact information of borrowers, lenders, homeowners, residents, and property agents. The type of information present in the dataset varies from person to person and includes some or all of the following: first and last name, residential and/or business address, email address and contact telephone number. The dataset also includes commentary about the property, relevant to its overall valuation.

There was some public reporting that the information disclosed included date of birth information. The Company advises that we do not collect nor was any date of birth information disclosed as a result of the Incident.

The Company is assessing the costs of the Incident and the subsequent reduction in revenue. The Company has cyber risk management and mitigation strategies in place which it has

implemented. LMW will provide an update to the market once the impact on earnings has been determined.

As part of our response, we have established a dedicated email mailbox privacy@lmw.com.au to respond to questions about this incident and have created a dedicated FAQ page (www.LMW.com.au/faqs) which we will continue to update. These FAQs are attached to this announcement.

We reiterate that LMW takes the privacy and security of our data very seriously and LMW will continue to work with any concerned parties. We thank our corporate partners, clients and shareholders for their patience and support during this challenging time.

John Wise
Company Secretary
(02) 8823 6300 email john.wise@lmw.com.au

About LMW

Founded in 1982 and listed on the Australian Stock Exchange in 2003, LMW has a long and proud heritage of providing independent professional property services to people and companies across Australia.

LMW has over 400 highly-skilled people and offers a wide range of services which includes commercial and residential valuations, research, and property advice with a focus in providing unrivalled property services that minimise the risks to our clients.

Data Disclosure Incident FAQs

Incident update as at 15 February 2019

We provide a substantive update below to all individuals who may be impacted by this incident. We are working closely with our lending clients to ensure that all potentially affected individuals are notified of this incident, so that they can take steps to prevent any potential misuse of their information.

In particular, we recommend that all potentially impacted individuals remain vigilant against a potential risk of receiving phishing and other spam communications from organisations purporting to be LandMark White or one of our lending clients.

Although LandMark White is one of the victims of this cybercrime, we take responsibility for this incident and deeply and sincerely regret that this incident has occurred. We remain committed to achieving the best possible outcome for all parties that may be impacted, and we are focused on supporting our partners and their customers in the wake of this incident.

Please continue to visit our website for information www.lmw.com.au/faqs.

Who is LandMark White?

LMW is an Australian property valuation and consultancy firm which was founded in 1982 and listed on the Australian Stock Exchange in 2003. We have a long and proud history of providing independent valuation services to Australia's leading banks and financial institutions, corporates and individuals. We employ 450 staff across Australia and are listed on the ASX with 99.7% of our shareholders in Australia.

What happened?

On 23 January 2019, we closed off a security vulnerability which we had identified in one of our valuation platforms. We have engaged leading privacy, digital forensic and cyber security consultants who have confirmed that the data disclosure relates to the vulnerability which had been secured. We can confirm that the disclosed dataset does not include loan application, date of birth, or other sensitive information.

What data is at risk?

The dataset contains property valuation and some personal contact information of borrowers, lenders, homeowners, residents, and property agents. The type of information present in the dataset varies from person to person, and includes (if provided): first and last name, residential and/or business address, email address, and contact telephone number. The dataset also includes commentary about the property, relevant to its overall valuation.

There is also a small subset of supporting documents relevant to the valuation assessment contained in the dataset, such as contracts for the sale of land, council rates, and strata reports. We are reviewing these documents to understand their contents and assess the potential privacy implications.

We reiterate that there is no evidence of misuse of any personal information, although we will continue to closely monitor for this together with industry partners.

What data is not at risk?

We can confirm that no loan application details, including financial and identity documents, are contained within the dataset. We can also confirm that no date of birth records, personal bank account details, payment or credit card details, username and password or other credentials, or other sensitive information exists in the dataset. We will provide further updates should this position change as the investigation continues.

Have you notified the Privacy regulator?

We have notified the Office of the Australian Information Commissioner of this incident. We will fully and transparently co-operate with their office in relation to this incident. You can visit the OAIC's website for more information at: https://www.oaic.gov.au.

Are your systems safe to use?

Independent security consultants have confirmed that the data was accessed via an exposed programming interface on one of our valuation platforms. We had already taken steps in January 2019 to block direct access to this interface to prevent any ongoing data disclosure, and it is no longer directly accessible from the internet. This has been validated by independent security consultants.

Additionally, although the evidence so far indicates that the incident was isolated to a single system, as a precaution, our external digital forensic specialists are performing in-depth continuous monitoring for any suspicious activity across our entire network, which has not detected any such activity.

Have I been affected?

At this stage, although investigations remain ongoing, LandMark White is adopting a very cautionary position and assuming that a subset of its valuation requests received by LandMark White during the period 4 January 2011 and 23 January 2019 may potentially be at risk. We are in the process of working with our lending clients to determine who is affected by this incident.

If you have received direct correspondence from your lender about this incident, it means that your information was likely contained in the dataset, and you should take steps to maximise the ongoing security of your personal information.

What actions do I need to take?

We are working with our major lending clients to understand the likely risk of harm that this incident poses for individuals whose information was contained in the dataset. Although the risk of harm may be considered low given that the information present in the dataset is not sensitive information and for the most part includes publicly available information, the best interests of potentially affected individuals whose information is contained in the dataset remains paramount.

We set out below practical steps that you should take to prevent any potential misuse of your information. We will update this advice, if necessary, as more information becomes known.

1. Remain vigilant to telephone call, SMS and email phishing scams requesting your personal details or the payment of money. Avoid opening attachments from unknown senders via email or social media. Ensure that any communications received from LandMark White or your financial institution in relation to this incident are legitimate.
   More information about phishing scams is available on the ACCC's website here: https://www.scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information/phishing.

2. You may also wish to contact your lender who you sought a valuation through to understand what protections they can put on your account to prevent any suspicious activity.
   We also recommend that as a matter of caution and good cyber risk hygiene, individuals can consider taking the following steps.

3. Review and continue to monitor your consumer credit report for any discrepancies or unusual activity. You can apply for an annual free credit report from each of the consumer Credit Reporting Agencies below. If you are not resident in Australia, you should contact your local Credit Reporting Agency or organisations such as IDCARE for further advice relevant to your circumstances.

CREDIT REPORTING AGENCY	WEBSITE
Equifax (formerly Veda)	https://www.mycreditfile.com.au/products-services/my-credit-file
Illion (formerly Dun & Bradstreet)	https://www.checkyourcredit.com.au/Personal
Experian	http://www.experian.com.au/consumer-reports
Tasmanian Collection Service	https://www.tascol.com.au/about-my-credit-file/

4. If you are concerned, you should consider requesting that a 'credit ban' be put in place while you investigate further. When a ban is put in place it 'freezes' access to your credit file and Credit Reporting Agencies are not able to disclose any personal information from your consumer credit file to any credit providers unless you provide written consent for them to do so, or if they are required by law. You are able to later lift this ban if you need to later apply for credit.

   You can find additional guidance about protecting your identity by visiting the OAIC's website here: https://www.oaic.gov.au/individuals/data-breach-guidance/what-to-do-after-a-data-breach-notification. You can also find additional guidance by visiting IDCARE's website here: https://www.idcare.org/learning-centre/fact-sheets.

Who is responsible for this incident?

An unknown criminal has maliciously accessed a LandMark White's system. We take our privacy obligations very seriously and are investing significant resources into investigating the source of the disclosure of the dataset. We have engaged leading consultants to help us understand this and will work with law enforcement and government security bodies as required.

Who has the data?

Although we do not know the identity of the individual, our investigations reveal that an unknown third party posted the dataset on a dark web forum on or about 11.57pm GMT, 31 January 2019, which has since been taken offline on or about 8.08pm GMT, 10 February 2019. We do not know how many people accessed the dataset throughout the approximately 10 days that it was available on the dark web.
We continue to investigate whether there were any previous disclosures made prior to this date. Further, we are scanning the internet for any potential further disclosure of personal information related to this incident so that we can take appropriate steps to protect individuals' interests should there be further disclosures.

We treat all threats to post further information very seriously and will continue to work with law enforcement and government agencies as necessary to investigate.

How many records were contained in the dataset?

Our investigations reveal that the dataset contains:

- approximately 137,500 unique valuation records, and approximately 1,680 supporting documents.
- approximately 250,000 individual records in total but a lot of records are duplicates.
- The date of the documents range between approximately 4 January 2011 and 20 January 2019.

We can confirm that the records contained in the dataset are a subset of the total number of records held by LandMark White in the valuation platform the subject of the incident. Our investigations into the scope of the disclosure continue, and we will continue to provide further relevant information as it becomes known.

How many unique individuals are affected?

We anticipate some affected borrowers will be notified by our lending clients of the incident commencing from today onwards. We continue to work with our lending clients to understand how many unique individuals are affected by this incident. This remains under close review as we are still reviewing the dataset in consultation with affected lenders.

Despite the fact that we have a large, cross-functional team working on this incident, this process may still take a number of weeks to complete and we appreciate your patience as we work with our lender clients about this. We have and will continue to expeditiously investigate this incident.

When did you first become aware of this Incident?

We have previously explained that on 4 February 2019, LandMark White first became aware that the dataset had been disclosed. As part of our ongoing investigation, we are continuing to identify further information and will continue to do so. We are committed to being open and transparent with all parties affected by this incident and will continue to update stakeholders.

We can now share that on 30 December 2018, we received a message through the 'Live Chat' messaging service on our website, providing us with a link to the dark web. As part of our standard

operating procedure, we investigated this and as we could not access the dark web link provided, at that time this was discounted as spam.

On 10 January 2019, our team received an email from the Australian Cyber Security Centre alerting us to a vulnerability. At that point in time, LMW was in the process of undertaking pre-planned systems upgrade work on the valuation platform the subject of the incident.
LMW also separately received a post from a user on our Twitter account at that time relating to data that we now know was publicly available on the dark web. Our Twitter account was not actively monitored over the holiday period, and we have only recently become aware of it.

The full extent of the incident was not apparent to us at the time of any of these communications, and we were not aware that there had been a disclosure of data at this time.

On 23 January 2019, we closed off internet access to the valuation platform the subject of the incident. We believe it was the closure of the access to the platform that prompted the disclosure of the dataset by the unknown third party.

Had we been aware of the full extent of the incident any sooner we would have immediately shut down access to the exposed programming interface. We sincerely regret that we did not act sooner and accept full responsibly for not having done so. We are committed to improving our processes and systems to ensure the ongoing strength and effectiveness of our cyber security and as part of our investigation into this incident, have and will continue to identify steps that we can take to improve our overall security position.

What is LandMark White's current trading position?

LandMark White acknowledges that this incident has affected many of our most valued clients, which we have been working closely with for over 35 years. We acknowledge that some lenders have, based on abundant caution, temporarily suspended our services while we work through this difficult time. This is to be expected in the circumstances while we support our partners and their customers in responding to the incident.

As a result of this, on 14 February 2019 we felt we needed to move into a market halt so we could get some clarity around what this incident means for our business. A large number of our clients have been incredibly supportive, fully understand the situation we face, and have continued the work flows in the face of this attack on our business. We thank them for their ongoing support during this difficult time.

It is important to work through this incident thoroughly with our corporate partners, financial institutions and affected customers, to re-establish trust in our organisation and to resume business activity as quickly as possible. We remain wholeheartedly committed to taking whatever steps are required to ensure that occurs.