PITCHER PARTNERS
ACCOUNTANTS • AUDITORS • ADVISORS

Level 22 MLC Centre
19 Martin Place
Sydney NSW 2000
Australia

Postal Address:
GPO Box 1615
Sydney NSW 2001
Australia

Tel: +61 2 9221 2099
Fax: +61 2 92231762

www.pitcher.com.au
partners@pitcher-nsw.com.au

Pitcher Partners is an association of independent firms
Melbourne | Sydney | Perth | Adelaide | Brisbane | Newcastle

15 August 2018

Consumer and Corporations Policy Division
The Treasury
Langton Crescent
PARKES ACT 2600

By email: regmod@treasury.gov.au

Dear Sir/Madam

Pitcher Partners' Business Recovery and Insolvency Division submission on Modernising Business Registers program (MBR Program)

Pitcher Partners' Business Recovery and Insolvency Division welcomes the opportunity to comment on the Modernising Business Registers program consultation paper of July 2018.

The MBR program sought submissions in the following four key areas:

- Attachment A – Flexibility of relevant legislation
- Attachment B – Enhanced Registry Services
- Attachment C – Funding Registry Infrastructure
- Attachment D – Director Identification Number (DIN).

This submission will address only the matters set out in Attachment D – Director Identification Number.

Preliminary Comments

The introduction of a Director Identification Number (DIN) is one part of a package of reforms to deter and penalise illegal phoenix activity. The need for a DIN is only one of several basic requirements missing from Australia's business and commercial environment. We believe that the introduction of DIN is unlikely to have a significant effect on the phoenix activities of rouge operators. There are a number of other benefits however, which strongly support the introduction of a DIN separate to considerations of 'illegal' phoenix activity.

The introduction of one small measure of corporate transparency needs to be assessed in the overall context of a package of other reforms needed to eradicate illegal phoenix activity. The MBR Program and this submission do not address these other reforms.

We provide the following commentary on Attachment D of the consultation paper:

Design Considerations

Q11. Design Consideration 1: Identity verification required to obtain a DIN

Currently, business structures can be easily established in Australia. However, it is easier to register as a director than it is to open a bank account. At present, when incorporating a company, an individual is only required to provide the Australian Securities and Investments Commission (ASIC) with:

- their name (at times not a consistent name);
- an address (which may or may not in fact be their address); and
- a date of birth (which may or may not in fact by the individual's date of birth).

The proposed director is not required to prove any part of their identity or disclose prior corporate history. What little information that is provided is not independently verified by ASIC.

This system is open to unethical behaviours such as the establishment of phoenix companies to avoid liabilities or other unethical business practices.

Although the MBR Program does not state how the DIN system will be administered, the Productivity Commission's *Business Set-up, Transfer and Closure* inquiry final report in December 2015 (**PC Report**) recommended that DINs be implemented by way of a low-cost one-off online registration on the ASIC website the first-time an individual takes up a directorship. Such registration would involve a 100-point proof of identity check (based on the identification requirements for opening a bank account). To manage the transition to a DIN, the PC Report recommended that for existing companies, existing directors be required to provide DINs to ASIC at the annual review date for the company, as a change to company details.

Process of Identity Verification

With the advent of technology, company officers or their authorised agents need a modernised system that allows them to deal with regulatory compliance more efficiently. We therefore believe if a DIN is introduced, the default should be an online identify proofing check to verify the identity of the company director. We have not considered in this submission whether an 'offline' alternative should be offered.

The level of identity verification required in obtaining a DIN is set out as follows:

	Digital Proof of Identity (DPOI)
First-time director	1. Use established verified account (i.e. MyGov); OR 2. Provide two forms of identification, one primary and one secondary through online identity verification process AND must meet condition standards: a) must have Australian residential address; AND b) sufficient data available in 3rd party databases to link the individual to the claimed identity
Existing director	Provide DIN in first annual return (or earlier) following introduction of DINs.

When obtaining, or being provided with a DIN, both new and existing directors would be subject to the identity proofing checks outlined above.

We make no comment on technology currently available or that might become available to perform the check but we are aware that the government, primarily through the Digital Transformation Agency but also led by the ATO, are developing the 'Trusted Digital Identify Framework'. The proposed matrix above assumes the current standard for establishing digital identity for online governments services, or proposed changes to identity proofing to obtain a reusable digital, could be simulated in the DIN application process.

If a first-time individual does not have an established verified account (i.e. MyGov), then the individual would be required to provide two forms of identification, one primary and one secondary, through an online verification process as part of the application for the DIN. They would also need to meet the condition standards outlined above. We consider that pseudonymous identities should not be supported in identity proofing check.

Contact details such as an email address and mobile phone number provided on a DIN application should be validated to establish a link between the individual and the device they are using to perform the identity proofing check. For example, the email address could be validated through an email confirmation method. The mobile phone number could be validated through a one-time PIN or SMS confirmation method.

Further, to meet its stated objectives, DIN information needs to be connected to not only newly incorporated and existing companies, but also to deregistered companies with which the director has been associated. We suggest that disclosure of deregistered companies forms part of the DIN application for individuals.

Existing directors would need to provide their DIN in their first annual return, or earlier by election. Existing directors would be subject to the same POI requirements as a first-time director. There will be at least a 12-month period of transition to allow existing directors to comply with the DIN requirements. It is highly likely that a proportion of existing directors will not comply with these requirements. The consequences of non-compliance could mirror the sanctions imposed on non-payment of annual return fees.

Once a DIN has been issued, that individual has satisfied the proof of identity requirements and would then have a reusable digital identity.

We have also considered that foreign directors should be subject to the same identity proofing requirements for example, Australian electronic visa record supported by both a primary and secondary form of identification.

Q12. Design Consideration 2: Obtaining consent

Currently, an individual must provide their written consent before being appointed as a director. The company keeps this consent. We believe that no change to this is required under the proposed DIN system. This consent could be required to be presented to ASIC with the proof of identity requirements under the suggested offline POI system.

For a first-time director, by proceeding with DPOI, the person consents for a DIN to be issued. For an existing director, the person consents to updates to the register by use of the DIN. We consider that the most effective way to ensure it is the authorised person themselves that is performing the function is via two-factor authentication (2FA).

We do not consider it appropriate to make statements on a software solution for 2FA, however we consider that the software should provide the process for correct authentication of the authorised individual and must require multi-factor authentication.

Q13. Design Consideration 3: DIN Application by Third Parties (Authorised Agents)

We have reframed design consideration 3 into the following series of questions and answers to isolate the issue of unauthorised consent by a third party:

1. *Does the 2FA consent process discussed above, offer sufficient security to prevent unauthorised consent by a third party?*

We note that *unauthorised consent* includes any update to the register i.e. new appointments, removals, and change of personal details not authorised by the individual.

The authentication process for first-time and existing directors under a 2FA scenario would include the following:

Individual	**Authentication requirements**
First-time director	1. User name and password; and 2. a) POI documents (where applicable); or b) Existing verified account (i.e. MyGov which uses multi factor authentication on login)
Existing director	1. User name and password; and 2. DIN; and 3. 2nd factor authentication

We consider it appropriate under a 2FA system, where identity proofing checks have been met that authorised agents be able to apply for a DIN on behalf of their clients.

If an agent, acting on behalf of an applicant, applies for a DIN, then the agent must provide all of the following:

1. evidence of the agent's authorisation to act for the applicant; and
2. evidence of the agent's identity and applicant's identity.

We do not comment on the form the agent's authorisation should take, save to say that the evidence provided by the agent to establish their authority to act as the applicant's agent in applying for the DIN should:

- be in writing
- be current
- state the full name of the applicant and the name of the agent
- set out the scope of the authority to act as the applicant's agent

Ongoing use of the DIN

One of the most important considerations for the use of DINs is to balance the risk of fraud and identity theft, with the ease of using the system. As outlined in the background to the formation of the MBR Program, there are 2.5 million registered companies, and over 2.9 million updates to the ASIC registry every year. Without security measures surrounding the ongoing use, the system will not achieve its stated objectives.

The most effective way of achieving the objectives is to require multi-factor authentication security each time the DIN is used as outlined in Q12 above.

Q14. Design Consideration 4: Availability of Data

The ASIC company register currently displays the following personal information about each director:

- Given names and family names
- All former given names and family names
- Date of birth
- Place of birth
- Residential address

We believe that data collected by ASIC falls into one of 2 categories as set out in the table below. The table provides a classification, access level and data inclusions for each category.

Category	Classification	Description	Access	Available data
1	Public	Public	Data that may be freely disclosed to the public	▪ Director's: - Name/former names/aliases - Date of birth (month & year only) - DIN - Electronic contact address - Residential address (if opt-in for publication) - Alternate address for service (if opt-out of residential address publication) - Registered address (e.g. company address or registered agent address) - Current and historical directorship and shareholding appointments (note that historical records would be 12-month transition or earlier by election for existing individuals) - Disqualification record
2	Private	Sensitive	1. Data that is not freely disclosed to the public 2. Government agencies' automatic access to data 3. Interested parties' access on application.	▪ Category 1 ▪ Residential address ▪ Full date of birth ▪ Place of birth ▪ Mobile phone number

We note that publicly available information is actually reduced under our proposed category 1 dataset above.

The datasets described above are already in the public domain. It is not confidential and all that is required in the first instance is collation from existing document lodgements. What is needed in the long term is better data collection as a whole.

Some of the regulatory and business benefits of ready access to data collected via a DIN are described as follows:

- Providers and users of data being able to engage with a single point of contact for the information collected from individuals and entities for regulatory purposes (at least for the key registers i.e. ABR, the Company Register and the Business Names Register). A single streamlined online system has the potential to interface with many more agencies for sharing of information than is considered in this submission.
- Efficient for directors of multiple companies to update their details on the companies register as they would only have to update one record.
- By capturing the relevant data through a common portal, this single point of contact can then share the data as required with the relevant registers that have differing data requirements.
- Address inconsistency in data between registers which has provided an opportunity for unethical business behaviour.
- Provide traceability of a director's relationships across companies to enable better tracking of directors of failed companies and prevent the use of fictitious identities.
- Liquidators are at the forefront of tackling phoenix activity. Often, they are hindered in their investigations by lack of documentary evidence and lack of funding. Free access to ASIC data (subject to conditions discussed below) is one way to assist liquidators in their investigations. In the absence of liquidator investigations, accurate identity information will assist regulators in locating and monitoring those individuals against whom enforcement action might be taken.
- Potential innovative uses of business register information by business and government.
- Increased ability for regulators to use data analytics to identify companies that are engaged in, or at risk of engaging in, illegal phoenix activity.
- Australia's current law reform focus (see Bankruptcy Amendment (Enterprise Incentives) Bill 2017) is aimed at '*reducing the stigma associated with business failure and striking a better balance between encouraging entrepreneurship and protecting creditors*', by reducing the default period of bankruptcy from three years to one. The privilege of reforms that assist in 'genuine' entrepreneurs who have tried and failed, need to be balanced with regulatory reform to assist in detecting the non-genuine where the intention is to exploit the corporate form to the detriment of unsecured creditors, including employees and tax authorities.

At present, checking ASIC registers only reveals information that has been given to ASIC by the directors and officers of this company. It is not verified and does not contain any meaningful information about the past corporate history of its directors.

While we anticipate some directors may be concerned about having their information linked using a DIN, for example, where it increases the risk of identity fraud, we counterbalance this argument by saying:

- There are fair and legitimate obligations attached to the creation of a corporate entity and a business register is the tangible requirement of transparency that comes with the privilege of using a limited liability company.
- There is a reasonable public expectation that following the incorporation of an entity, the name and basic contact details of those connected with the incorporated entity be made available to the public.

- It is essential that an entity's stakeholders can identify the parties involved in an entity, however accurate and up-to-date data is useful for reasons beyond this. Registers can also be used to gather intelligence to combat fraud and financial crime. It is therefore important that the current review of the content (and role) of maintaining business registers demands public interest and transparency over the maintenance of privacy of directors.

We will not be commenting in this submission on any costs associated with accessing the above data, save to say that the current costs associated with accessing ASIC records is prohibitive and runs contrary to the principles of public interest and transparency outlined above.

Interested parties on application

We recommend that access to category 2 (outside of government agencies) should be granted to specified organisations or individuals in certain circumstances. This may be through application to ASIC for defined or public interest purposes. The criteria around who can request this information would need to be clear. We consider that a 'defined' purpose would include the appointment of an external administrator to the entity and 'public interest' purposes would include creditors, shareholders, journalists or legal professionals. Further comments particular to the director's residential address are provided below.

We note that the PC Report recommended that *'there should be no lessening of the existing recording of, and means of accessing, director information'*. We address both this comment and design consideration number 4 through the following series of questions and comments:

1. *Under the existing register, what is the purpose of a director's residential address being made publicly available?*

We see two reasons for this.

The first is that the residential address provides an additional data point to distinguish between individuals, as addresses are largely unique to an individual.

The second is that the residential address provides a mechanism for third parties to contact the director independent of the company (i.e. for service of documents).

2. *What are the concerns for publication of the director's and other company officers' addresses?*

The concerns for the individuals themselves are privacy, safety and security, and fraud.

The concerns for third-party users of the system is accuracy. As there are currently separate entries for each company, the residential address is a unique identifier to assist in mapping a director's corporate involvement.

3. *Could the DIN perform the same function as the residential address?*

Yes. The DIN connects companies through shared directors and the user would not have to search multiple variations of the same name to ensure accuracy.

We consider that a DIN would perform much of the functionality as the publication of directors' residential addresses and if a DIN is introduced, there is minimal justification for also having directors' residential addresses publicly available. Further, there is less need for public access to the directors' residential addresses to support the accuracy demanded by third party users when measured with the increased identity verification process involved in acquiring a DIN.

Some education would be required for interested parties (i.e. creditors, shareholders or legal professionals) in how to obtain the DIN from the individual. For example, updates to suppliers' credit application to include disclosure of the DIN as a requirement.

4. *Does the DIN address the use of the residential address as discussed in Q1.?*

No. The DIN only addresses the use as an additional data point and does not address its use as a mechanism for third parties to contact a director independent of the company.

Our solution is addressed in the data categories listed above. The director would be required to provide a usual residential address that would only be available under category 2 access, unless the director chooses at the time of the DIN application to consent to this information being publicly available. If the director chooses not to have this information made publicly available then the director would be required to include an address for service (in lieu of their residential address) for publishing in category 1.

Currently pursuant to s.205D of the Corporations Act 2001, an individual must provide their residential address unless they are entitled to have an alternative address substituted for their usual residential address by meeting certain criteria. We consider an additional criterion be added to s.205D to the effect of 'the person has not consented to have their usual residential address published on the register'. We consider that the Application to use an alternative address (form 378) would no longer be required.

The status of the alternative address as an address for service under ss.109X(2) of the Corporations Act remains unchanged.

The requirement that a post office box address is not an acceptable alternative address remains applicable.

5. *Should the change in approach of residential address be applied to other company officers?*

Yes, in certain circumstances. The change in approach must also be applied to shareholders' residential address publication where the individual is the same.

6. *Are other changes to the existing law required?*

- We submit that no change to existing section 201D of the Corporations Act 2001 is required for the reason that concerns of ease of access to this information appears to focus on electronic means and not information held by the company at its premises.

- We consider that an offence would need to be introduced in the Corporations Act 2001 for directors that knowingly apply for more than one identification number or provide false information to ASIC. We do not propose to discuss possible sanctions in this submission.
- Currently, there are anomalies around the timeframes for changes to be made or lodged with ASIC which should be corrected on the introduction of a DIN. For example, lengthy timeframes for changes to company details might be desirable in a paper based system but with only one record to update under a DIN system, we argue that these lengthy time frames are excess and should be reduced.

7. *How do ASIC (and other agencies) deal with historical documents that include the residential address?*

It is understandable that third party websites have their own data sets which may include the residential address. This means that even if directors' addresses are not publicly available in category 1, it would not necessarily affect the existing information available on external websites. As ASIC does not have control over these websites, this means that directors' residential addresses may still be publicly assessable online.

For the information that ASIC does control, directors' residential addresses can be found in documents attached to a company's record on the ASIC register. We consider that being able to identify each instance of an address and redact this information would be such an expensive and resource intensive task that the change should not be retrospective and would not affect the historic documents on record.

The status quo assumes ASICs application of suppression of residential address (Form 379) remain unchanged for historical documents.

8. *How is access to the directors' residential address administered?*

Our proposed data classification scheme assumes that ASIC would continue to collect the directors' residential address, regardless of if the information is provided in category 1. We also consider the possibility of giving others access to directors' residential addresses and the circumstances in which access may be provided, specifically through category 2.

We agree that there may be instances where legitimate interested parties need to contact a director where:

a) they have been unable to contact a director through their published address for service; and

b) they have been unable to contact a director through their company;

and where only one of these circumstances is satisfied and

c) the interested party has reason to believe that the company or a third party is intercepting the correspondence then;

that interested party should be able to apply to ASIC for access to a director's residential address.

Interested parties could include creditors, shareholders or legal professionals.

Government agencies would have automatic access to the residential address. We recommend that an entity entering a form of external administration would be a 'defined' purpose such that the external administrator would have access to category 2 information triggered by the lodgement of the Form 505 – Appointment of External Administrator.

Conclusion

It is evident that all government registers require review. The introduction of DIN is an essential part of the modernisation of Australia's business registers.

We support the introduction of a DIN. While it will not eradicate illegal phoenix activity, it will support existing measures to tackle the problem.

Should you have any queries in relation to this submission, please do not hesitate to contact me on [redacted]

Your Faithfully
PITCHER PARTNERS

PAUL GERARD WESTON
National Chairman
Business Recovery and Insolvency Services