

2 July 2015

T +61 2 9223 5744 F +61 2 9232 7174

E info@governanceinstitute.com.au

Level 10, 5 Hunter Street, Sydney NSW 2000

GPO Box 1594, Sydney NSW 2001

W governanceinstitute.com.au

Business Set-up, Transfer and Closure
Productivity Commission
GPO Box 1428
Canberra ACT 2601

By email: business.inquiry@pc.gov.au

Dear Commissioners

Business Set-up, Transfer and Closure: Draft Report

Governance Institute of Australia is the only independent professional association with a sole focus on whole-of-organisation governance. Our education, support and networking opportunities for directors, company secretaries, governance advisers and risk managers are second to none.

Our members have primary responsibility to develop and implement governance frameworks in public listed, unlisted and private companies. They frequently are those with the primary responsibility for dealing and communicating with regulators such as the Australian Securities and Investments Commission (ASIC), and in listed companies have primary responsibility to deal with the Australian Securities Exchange (ASX) and interpret and implement the Listing Rules. Our members have a thorough working knowledge of the operations of the markets and the needs of investors, as well as compliance with the *Corporations Act 2001* (the Act). We have drawn on their experience in our submission.

We have responded only to the following matters set out in the Draft Report:

- Corporate restructuring processes
- Protecting against phoenix activity

Corporate restructuring processes

Governance Institute members accept that there could be instances where the risk of personal liability for trading while insolvent leads directors to appoint external administrators prematurely in circumstances where a work-out managed by the directors and the company might ultimately lead to a better outcome for shareholders, creditors and employees.

Governance Institute also considers that any reforms to directors' personal liability for insolvent trading should not be made at the expense of innocent creditors, employees, customers and suppliers who deal with a company in good faith on the assumption that the company is solvent. Any reform of the law that is applied to directors' duties in regard to insolvent trading should not be at the expense of creditor protection.

While the defences in s 588H currently operate well to ensure that there is a balance between taking sensible commercial risks and the protection of creditors, we accept that the manner in which the *Corporations Act 2001* (C'th) imposes personal liability on directors for debts incurred by their company while it is insolvent can take effect in two ways that work against restructuring.

Firstly, the liquidator of an insolvent company can sue a director for the debts incurred by the company while it was insolvent. Secondly, because the duty to prevent insolvent trading is both a civil penalty provision and a criminal penalty provision, it can be enforced by the regulator, the Australian Securities & Investments Commission (ASIC).

If a director breaches the civil penalty provision, the penalties which the court can impose include disqualifying them from managing a company for a specified period of time, or paying a penalty of up to \$200,000, or paying compensation to the company. If the additional element of dishonesty is made out, then under the criminal penalty provisions, the director could be fined up to \$200,000 and imprisoned for up to five years.

Governance Institute is therefore in support of Draft Recommendation 15.2 that:

The Corporations Act 2001 (Cth) should be amended to include provision for a 'safe harbour' to allow companies and their directors to explore restructuring options without liability for insolvent trading. During such a period, the directors would retain control of the company, but receive independent advice from registered advisers.

- Advisers appointed in safe harbour would be disqualified to act as administrators, receivers or liquidators in any subsequent insolvency process for the company.
- The company would be required to inform ASIC, and ASX in the case of listed companies, of the appointment of an adviser.
- In informing themselves and the adviser, and determining whether to act on any restructuring advice, directors would be under a duty to exercise their business judgment in the best interests of the company's creditors as a whole, as well as the company's members.
- If the positive thresholds above are met (and evidenced), a director's duty not to trade while insolvent would be considered to be satisfied during the period of advice and for actions directly related to implementing the restructuring advice.

Governance Institute strongly supports the concept of an informed market and is of the view that providing information to existing and potential creditors should be a foundation stone of any approach to the insolvent trading laws. Disclosure provides creditors with the opportunity to decide their course of action. For example, creditors could well be interested in a work-out and extending further credit. Conversely, creditors could take the view that the current directors are fatal to the ongoing viability of the company.

We therefore support Draft Recommendation 15.2 on the basis that the directors have the support of their creditors and remain in discussion as to the extension of credit.

We note that Draft Recommendation 15.2 is not dissimilar to the 'moratorium' proposed in a Treasury consultation paper on this issue in 2010 (*Insolvent Trading Safe Harbour Options Paper*).

During that consultation, we noted that listed companies are already subject to a continuous disclosure regime, and therefore if a company is approaching insolvency, it will be required to disclose such price-sensitive information to the market. A moratorium would see both listed and unlisted companies subject to a full disclosure requirement. We noted that such disclosure could see creditors unwilling to extend credit.

We expressed the view — and continue to hold to it — that a mechanism will need to be considered for advising those who deal with the company that it is in a moratorium (which word we will use for the proposed amendments to the Corporations Act as set out in Draft Recommendation 15.2).

Under the current law, a company is required to notify ASIC and place a notice on its letterhead that it is in administration, which is the mechanism to ensure that all those dealing with the company know its financial position. Governance Institute submits that there should be a similar obligation on a company whose directors wish to take advantage of the proposed amendments to the Corporations Act as set out in Draft Recommendation 15.2. Consideration could be given as to whether the directors should also be required to convene a meeting of creditors at an early stage of the process to discuss the proposed restructuring.

We also note that the moratorium as proposed in Draft Recommendation 15.2 would not prevent secured creditors taking action to enforce their security or unsecured creditors commencing proceedings to recover amounts owed to them or for the winding up of the company.

We also recommend that any amendments to the Corporations Act to progress Draft Recommendation 15.2 be subject to public consultation.

Protecting against phoenix activity

Draft Recommendation 15.8 is that:

Section 117 of the *Corporations Act 2001* (Cth) should be amended to require that, at the time of company registration, that directors must also provide a Director Identity Number (DIN).

A DIN should be obtained from the Australian Securities and Investments Commission (ASIC) via an online form at the time of an individual's first directorship. In order to obtain a DIN individuals should be required to provide 100 points of identity proof, and verify that they have read brief materials on directors' legal responsibilities provided as part of the online registration.

For existing companies, their directors should be required to obtain a DIN. The director DINs should then be provided to ASIC at the annual review date for the company, as a change to company details. To enforce these requirements, ASIC should be empowered under section 205E of the *Corporations Act 2001* (Cth) to ask a person who is a director to provide their DIN.

We strongly support this recommendation.

While the Draft Report focuses on this recommendation as a means of eliminating the problem of fictitious identities being used for company directorships when new companies are registered, which can support phoenix activity, we note there are multiple other benefits to this recommendation.

In January of this year, Governance Institute wrote to Treasury about the need for a DIN to be introduced as a means of mitigating the risk posed to directors and officers, as a result of personal information that can be readily used for identity theft or for assaults on personal security being publicly available on the ASIC register of officeholders.

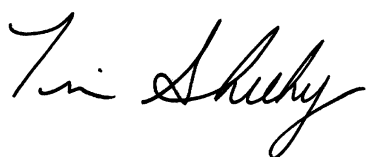
We have attached our letter to Treasury on this matter, which sets out:

- the risks
- why the current legislative requirements give rise to those risks
- how the objectives of the current public policy have been distorted by changes in technology, given that the advent of technology on a global scale has fundamentally altered the capacity to access any personal information held on an individual on a database
- how the objectives of the public policy can be retained through the introduction of a DIN

- the state of play in other jurisdictions
- the importance of this reform being implemented as soon as possible in light of the tender for the sale of the ASIC registry business having commenced.

That is, the introduction of a DIN will certainly facilitate ASIC being able ‘to “join the dots” between multiple failed companies so that the regulator can investigate phoenix activity more readily, with a view to banning a person with a consistent history of insolvent companies from managing any further companies” (as expressed eloquently by Associate Professor Helen Anderson, Professors Ian Ramsay and Ann O’Connell and Associate Professor Michelle Welsh in their submission on the December 2014 Issues Paper). Equally, it would also protect honest directors and officers from the risk of identity theft and assaults on personal security.

Yours sincerely

A handwritten signature in black ink, reading "Tim Sheehy". The signature is written in a cursive, flowing style.

Tim Sheehy
Chief Executive

6 January 2015

Diane Brown
Principal Advisor
Corporations & Capital Markets Division
The Treasury
Langton Crescent
PARKES ACT 2600

Dear Diane

Public display of personal information of officeholders

I am writing to express the increasing concerns raised by many of our members in relation to the risk posed to directors and officers as a result of information that can be readily used for identity theft or for assaults on personal security being publicly available on the ASIC register of officeholders. We outline these risks on the following page.

Governance Institute strongly supports the requirement that an officeholder provide personal information to the regulator. This information allows the regulator to take action should the officeholder be in breach of their duties. We also strongly support the public policy that other persons too may need to accurately identify and locate individuals who are officeholders of companies in connection with the protection and enforcement of their personal rights and liabilities.

However, the advent of technology on a global scale has fundamentally altered the capacity to access any personal information held on an individual on a database. How an organisation collects, uses, discloses and otherwise handles personal information is subject to the *Privacy Act 1988* and an organisation must secure the private information it holds. Generally, only authorised personnel are permitted to access the personal details of individuals. While we recognise that the information held on the ASIC register fulfils a different role than that held on other individuals on many other databases, the security of personal information remains relevant.

Current law

The current provisions in the Corporations Act 2001 require public disclosure of personal information about directors and officers of a company registered under the Act. In particular, s 1274(2) of the Corporations Act requires that ASIC must allow certain persons to inspect documents lodged with ASIC. These documents include application for registration of a company and notices containing details of directors and company secretaries. In turn, ss 117 and 205B of the Corporations Act require the following information about directors and company secretaries be disclosed in those documents:

- given names and family names
- all former given names and family names
- date of birth
- place of birth
- residential address.

Accordingly, the ASIC public register displays this personal information about each officeholder.

ASIC does not have the power to exempt persons from, or modify, ss 117 or 205B or the provision in s 1274(2) relating to the right to inspect documents. ASIC is also obliged to keep and maintain such registers in such form as it thinks fit (s 1274(1)) and must consider that the information contained in these registers is mandated under the Corporations Act to be made publicly available.

Section 205D of the Corporations Act is the only basis on which this information can be altered, where officeholders have concerns for personal safety. Under s 205D a person is entitled to have an alternative address substituted for their residential address if:

- their residential address is not on the electoral roll for personal safety reasons, or
- their name is not on an electoral roll and ASIC determines that including their residential address would put at risk their personal safety or the personal safety of members of their family.

Concerns regarding risk of identity theft

Identity theft is feasible if an individual intent on the crime has access to the given and family name, date of birth, residential address and place of birth of another individual. As such, all officeholders on the ASIC public register are at a heightened risk of identity theft.

When associated with identity fraud, identity theft can result in victims experiencing serious negative consequences, including financial loss, inconvenience and in some extreme cases, severe trauma. Governance Institute is of the view that our regulatory framework should not expose our directors and company secretaries to such a risk.

Concerns regarding personal safety

Our concern extends beyond identity theft to the issue of the personal security of senior officers. The companies with which they are involved may provide some level of security to high-profile CEOs and their families, but this is significantly undermined when their residential address is a matter of public record. Furthermore, as interest in the environmental and social impacts of companies continues to increase, a wide range of individuals can become interested in pursuing 'causes' by confronting directors and officers at their homes. For example, recently members of a trade union picketed on the front law of the chair of Aurizon Ltd as they disagreed with a company decision on an industrial relations matter. The picketers noted they had sourced the residential address of the chair from the ASIC public register.

As noted above, in the event of concerns regarding personal safety, it is currently possible for officeholders to obtain a 'silent enrolment' from the Australian Electoral Office which can be used by an officeholder to seek the withholding of publication of their residential address by ASIC, with the address of the company nominated instead on the public register. Of course, in such situations, ASIC retains access to the residential address of the officeholder, which is entirely proper, and information concerning the usual residential address may be disclosed to a court for the purposes of enforcing a judgment debt ordered by the court.

Notwithstanding this, while it is possible for an individual to apply to have their residential address details suppressed on ASIC's public register because of safety concerns, the issue we are raising is one that touches every officeholder whose details are on the ASIC register.

Moreover, any legacy system will hold the information of officeholders whose personal details have been registered over many years and in relation to multiple companies. In a world where electronic information remains traceable and accessible, even if no longer posted, such information remains 'live', available and therefore readily accessible, irrespective of an individual's changed status.

Intersection of public policy with a world changed by technology

Governance Institute is of the view that it is entirely appropriate that ASIC request and retain the personal details of all officeholders on a database subject to strict controls and access.

However, we are also of the view that the open publication of birthdates and birth places of officeholders serves no useful purpose other than for persons with criminal intent. In this world of increasingly faceless transactions, birthdates have unfortunately become by default the first form of identity check by banks, telecommunications companies and other institutions to ascertain that they are communicating with an authorised person. To make readily available the personal information of the business community's most influential officeholders is fraught with risk and a significant magnet for cyber-criminals.

The law requires a director to be 18 years of age. Date of birth is therefore essential to accurately identify if a person consenting to be a director meets the statutory requirement. A date of birth may also be useful in correctly identifying officeholders who share the same name, for example, John Smith. When date of birth is triangulated with place of birth, correct identification is assured.

However, while date of birth and place of birth are necessary to ensure correct identification by the regulator as to one particular officeholder being involved with one company rather than another, neither date of birth nor place of birth are necessary should an individual need to locate an officeholder to enforce rights and obligations if the triangulation has already been undertaken by the regulator. The address is required in this instance.

The issue therefore becomes one of ensuring that the public policy test is met while not putting officeholders at risk of identity theft or infringement of their personal safety.

Recommendations for reform that meet the public policy test

Governance Institute is of the view that technology provides a solution to the accurate identification and location of officeholders should either the regulator seek to take action if the officeholder is in breach of their duties or any individual seek to locate an officeholder in connection with the protection and enforcement of their personal rights and liabilities.

We recommend that a unique ID be introduced by ASIC for each officeholder.

ASIC currently uses a code to suppress the address of a director if they have gone through the Electoral Commission process for a 'silent enrolment's, so some thought has already been given to the use of technology to identify an officeholder.

The assignation of a unique identification code (ID) for each officeholder would:

- ensure that the regulator continued to hold all of the personal information required to correctly identify an officeholder and their connection to any particular company or companies (including legacy information)
- remove the risk of identity theft which is currently posed by the public display of personal information of officeholders, given that identity theft is facilitated greatly by the provision of date of birth, place of birth, full and former names and residential address.

One key business efficiency advantage of unique officeholder IDs that could be explored by ASIC, consistent with ASIC's deregulatory initiatives¹, is that this initiative should allow an officeholder to submit a single change of family name or change of address (residential or

¹ Refer ASIC Report 391, *ASIC's deregulatory initiatives*, May 2014 (Para 1) in which it is stated that ASIC's mandate is to 'strive to reduce business costs and administer the law effectively with a minimum of procedural requirements'.

service address) to their ID data, which could then flow through to update all of the companies of which this person is or was an officeholder. It is highly inefficient for officeholders on multiple companies (especially entities with multiple subsidiaries) to have to lodge this same information over dozens, and sometimes hundreds of companies.

Any individual seeking to locate an officeholder to enforce rights and obligations could locate the officeholder they seek through the use of the officeholder ID. Any search would be conducted by using the name of the officeholder and company. It would be rare for two directors with the same name to serve on the board of one company, although it is possible. For example, currently there are two Mark Johnsons serving on the board of Westpac. However, given that the individual would be seeking to locate all officeholders of the one company, this would not be a concern.

Other parties are also interested in identifying and at times locating particular officeholders, as they seek to assess who has an interest in particular companies. Such third parties include the media, lawyers, banks and other creditors, liquidators and real estate firms. The use of an officeholder ID would assist this, as it would assist any individual seeking to locate an officeholder, as the ID held by the officeholder would reveal all of the companies with which they are involved. There are advantages to linking officeholders in this way, both for the regulator and those seeking to locate individuals in connection with the protection and enforcement of their personal rights and liabilities.

We also support the need for a mechanism to be publicly available in order to serve documents on officeholders. If an officeholder ID is used, there would need to be an obligation on each officeholder to provide a service address. However, the public generally does not need access to the residential address of officeholders.

We recognise that legacy data will probably not be able to be dealt with. Existing records of officeholders' personal information embedded in a vast number of documents filed with ASIC and displayed on the public register will still be available as it would be wholly impractical for such information to be removed. The UK tried to contain the problem when it moved away from the public display of residential addresses by removing data only upon application. We would recommend a similar approach in Australia.

Other jurisdictions

It is of interest to consider the statutory obligations for the public display of personal information of officeholders in other jurisdictions. Assessing whether less personal information is required to be publicly displayed in other jurisdictions, and whether this has any negative impact on the capacity of regulators to take action or officeholders to be located as appropriate, is useful in considering if changes to our statutory framework are feasible.

The detail of requirements in other jurisdictions is set out in Appendix 1, including in a matrix in which all requirements can be easily compared.

It is clear from consideration of other jurisdictions Australian officeholders are far more exposed than their international counterparts in terms of their general right to privacy, personal safety and security.

Scoping study into the sale of the ASIC registry business

The proposed sale of ASIC's registry business highlights further the issues we have raised in this letter. Issues of data control, security and assurance will need to be considered in relation to the sensitive information currently held on the ASIC register.

There could be strong commercial interest in the personal information contained on the register. Information that is compelled by statute in order to ensure that the regulator can take action

should an officeholder be in breach of their duties or to assist individuals in connection with the protection and enforcement of personal rights and liabilities has been provided for reasons of public policy, however, and has not been provided for commercial application. It is important that any such information be collected for regulatory reasons, but it should not be made available publicly for the reasons set out above or for commercial application, as this would be a fundamental breach of privacy and a misuse of the rationale for the public policy.

Conclusion

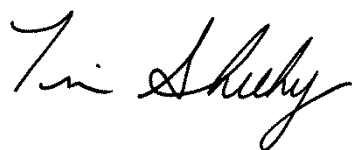
Governance Institute recommends that:

- ASIC retain the personal details of all officeholders
- ASIC issue each officeholder with a unique identification code
- the ASIC public register not display the date of birth, residential address and place of birth of officeholders, but the officeholder name, unique identification code and a service address.

Governance Institute recognises that amendments to the Corporations Act would be required to facilitate these reforms. Governance Institute also recognises that public consultation would need to be undertaken with stakeholders on any such reforms.

We would be more than happy to meet with you to discuss this matter.

Yours sincerely

A handwritten signature in black ink that reads "Tim Sheehy". The signature is written in a cursive, flowing style.

Tim Sheehy
Chief Executive

T +61 2 9223 5744 F +61 2 9232 7174
E info@governanceinstitute.com.au
Level 10, 5 Hunter Street, Sydney NSW 2000
GPO Box 1594, Sydney NSW 2001
W governanceinstitute.com.au

Appendix 1: 2014 Comparison of information obtained by regulators and made available to general public

Table 1: 2014 Comparison of information obtained by regulators and made available to general public

| | Information provided to the Companies office | | | | | Information shown on the public register | | | | |
|---------------------------------------|--|----|---------------------|---|-------------|--|----|--|---|------------|
| | Australia | NZ | UK | USA + | Sth Africa | Australia | NZ | UK | USA | Sth Africa |
| Full name | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Former names | ✓ | - | - | - | - | ✓ | - | - | - | - |
| Date of birth | ✓ | ✓ | ✓ | No | ✓ or ID | ✓ | No | ✓ <i>*(under review)</i> | No | ✓ or ID |
| Place of birth | ✓ | ✓ | Nationality only | No | No | ✓ | No | Nationality only | No | No |
| Residential address | ✓ | ✓ | ✓ | No (May show work addresses or PO boxes on forms lodged) | No | ✓ @ | ✓ | Can opt for 'service address' in place of residential address on public register # | No (May show work addresses or PO boxes on forms lodged) | No |
| Occupation | | | ✓ | | | | | ✓ | | |
| Passport ID required for non-citizens | | | | | ✓ | | | | | No |
| Officeholder ID code | | | Under consideration | | Or Passport | | | | | |

| | | | | | | | | | | |
|----------------------|--|--|--|--|----|--|--|--|--|----|
| | | | | | No | | | | | |
| Phone/mobile numbers | | | | | ✓ | | | | | No |
| Email addresses | | | | | ✓ | | | | | No |

* UK — publication of full date of birth currently under review

+ USA — two-tier system. Some state regulators require more information, but it is not made publicly available.

UK — if residential address not on public register, public authorities and credit reference agencies may apply to the Companies Office for access to the residential information and access is only granted subject to meeting certain criteria.

@ Australia — can only be removed if there are 'personal safety' issues and if not shown on electoral roll.

New Zealand

The given and family name and residential address is displayed on the public register, but not the date of birth or place of birth.

United Kingdom

Under UK corporate law, the following information must be lodged with Companies House in respect of every director:

- Full name (all given and family names, but no former names)
- Date of birth
- Nationality (but not place of birth)
- Occupation
- Usual residential address
- Country of residence.

However, any person being appointed can opt to have a 'service address' for all communications. Under the UK Companies Act 2006, every director is given the option of providing a service address for the public record with the residential address being kept on a separate record to which access is restricted to specified public authorities and credit reference agencies, which must apply to Companies House for access to the register. Access is only granted after applications have been vetted and if they meet specific criteria set out in legislation. Details of the legislation can be found at http://www.legislation.gov.uk/ukxi/2009/214/pdfs/ukxi_20090214_en.pdf.

The requirement to file the company secretary's residential address has been abolished.

The Small Business, Enterprise and Employment Bill is currently going through the Parliamentary process. One of the proposals therein (s 84) is that the day (but not the month or year) of a director's birth will not be public.

There are concerns that this will be ineffective, and interest has been expressed in our idea of an officeholder identification code.

South Africa

- The Companies Act (s 24(5)) requires all companies to maintain a record of directors reflecting full name, date of birth or ID (passport number if not a citizen of the Republic of South Africa). Addresses are not required. This register is open to inspection by securities holders free of charge and any member of the public on payment of a fee (s 26)).
- Companies are required to supply to the regulator [CIPC] the telephone numbers (landline and mobiles) as well as email addresses, when notifying appointments/changes of directors. The regulator has insisted on this to enable them to contact the directors directly when the company's agent notifies changes to the regulator. This is a fraud prevention measure to prevent company 'hijacking'. However, public disclosure by the regulator of its records **excludes** director contact details and conceals certain aspects of director ID numbers to ensure privacy.

United States

The US has a two-tier regulatory model. Securities laws are enforced by the Securities Exchange Commission (SEC) at the federal level and laws governing companies are enforced at an individual state level by state-based regulators.

Officers and directors of public companies in the US are not required to submit their place and date of birth to the SEC, nor are they required to do so under company law in the State of Delaware (where over half of all US companies are incorporated) or any other significant US state jurisdiction.

The only public information about directors and officers is their age and work history, which is contained in the proxy statement (the US version of the notice of meeting). Addresses on other filings, such as under Section 13 of the Securities Exchange Act reporting ownership over five per cent of a company's shares (the US equivalent of Substantial Shareholder Notices), are usually work addresses or PO boxes.

Directors of insurance companies regulated by individual states are required to disclose more detailed information to their state regulators, including their date of birth and other personal information for the purpose of the state vetting them. Similar provisions exist for state bank directors and other highly regulated industries. However, none of this information is made public.

24 September 2015

General Manager
Deregulation Division
The Treasury
Langton Crescent
PARKES ACT 2600
Email: deregulation@treasury.gov.au

Dear Minister Frydenberg

Treasury Legislation Amendment (Spring Repeal Day) Bill 2015

Governance Institute of Australia is the only independent professional association with a sole focus on whole-of-organisation governance. Our education, support and networking opportunities for directors, company secretaries, governance advisers and risk managers are second to none.

Our members have primary responsibility to develop and implement governance frameworks in public listed, unlisted and private companies. They frequently are those with the primary responsibility for dealing and communicating with regulators such as the Australian Securities and Investments Commission (ASIC) and Australian Taxation Office (ATO) and in listed companies have primary responsibility to deal with the Australian Securities Exchange (ASX) and interpret and implement the Listing Rules. Our members have a thorough working knowledge of the operations of the markets and the needs of investors. We have drawn on their experience in our submission.

Governance Institute supports the Treasury Legislation Amendment (Spring Repeal Day) Bill 2015 which will make the Australian Business Number (ABN) the single numerical identifier for companies registered under the Corporations Act from 1 July 2016 and the amendment of taxation laws to allow an entity with an ABN to use that number instead of a Tax File Number (TFN).

We are of the view that combining the ABN, Australian Company Number (ACN) and TFN so that there is a single numerical identifier — the ABN — for a corporate entity will simplify compliance arrangements for companies in Australia.

We also believe that it will facilitate Standardised Business Reporting (SBN) on a prospective basis, as it consolidates the numbers used to identify corporate entities.

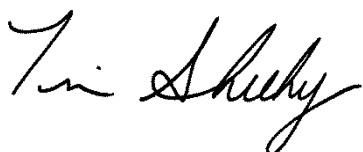
Furthermore, from a contractual point of view, it facilitates the identification of corporate entities in future, which we support. Our members view this as an easing of the compliance burden.

The bill means that a company will no longer be able to register using its ACN as the company name and we also support this proposition.

Our one note of caution relates to the need to ensure that the proposed legislative amendments keep the TFNs of those individuals involved with corporate entities entirely separate from the combined ABN, ACN and TFN of the corporate entity. We would also stress the importance of having an appropriate transition period to assist entities in relation to the implementation of the change.

Governance Institute notes that it is extremely important that the requirements to secure and protect the TFNs of individuals be maintained. In combining the ABN, ACN and TFN of corporate entities, it is vital that the confidentiality of individuals' TFNs be maintained, in order to mitigate against identity theft and preserve the privacy of individuals.

Yours sincerely

A handwritten signature in black ink that reads "Tim Sheehy". The signature is written in a cursive, flowing style.

Tim Sheehy FGIA
Chief Executive

23 July 2014

John Price
Commissioner
Australian Securities & Investments Commission
Level 24
120 Collins Street
MELBOURNE VIC 3000

T +61 2 9223 5744 F +61 2 9232 7174
E info@governanceinstitute.com.au
Level 10, 5 Hunter Street, Sydney NSW 2000
GPO Box 1594, Sydney NSW 2001
W governanceinstitute.com.au

Dear John

Potential risk of identity theft for directors and officers in relation to information about them on ASIC's register of officeholders

I am writing to express the concerns raised by our Members in relation to the risk posed to directors and officers as a result of information that can be readily used for identity theft or for assaults on personal security being publicly available on the ASIC register of officeholders.

Governance Institute strongly supports the requirement that an officeholder provide personal information to the regulator. This information allows the regulator to take action should the officeholder be in breach of their duties.

However, the advent of technology on a global scale has fundamentally altered the capacity to access any personal information held on an individual on a database. How an organisation collects, uses, discloses and otherwise handles personal information is subject to the *Privacy Act 1988* and an organisation must secure the private information it holds. Generally, only authorised personnel are permitted to access the personal details of individuals. While we recognise that the information held on the ASIC register fulfils a different role than that held on other individuals on many other databases, the security of personal information remains relevant.

The ASIC register contains the following personal information about each officeholder:

- date of birth
- residential address
- place of birth.

Identity theft is feasible if an individual intent on the crime has access to the date of birth, residential address and place of birth of another individual. As such, all officeholders on the ASIC register are at a heightened risk of identity theft. When associated with identity fraud, identity theft can result in victims experiencing serious negative consequences, including financial loss, inconvenience and in some extreme cases, severe trauma. Governance Institute is of the view that our regulatory framework should not expose our directors and company secretaries to such a risk.

Our concern extends beyond identity theft to the issue of personal security of senior officers. The companies with which they are involved may provide some level of security to high profile CEOs and their families, but this is significantly undermined when their residential address is a matter of public record. Furthermore, as interest in the environmental and social impacts of companies continue to increase, a wide range of individuals can become interested in prosecuting 'causes' by confronting directors and officers at their homes, as has happened in the United Kingdom.

In the event of concerns regarding personal safety, it is currently possible for officeholders to obtain a 'silent enrolment' from the Australian Electoral Office which can be used by an officeholder to seek the withholding of publication of their residential address by ASIC, with the address of the company nominated instead on the public register. Of course, in such situations, ASIC retains access to the residential address of the officeholder, which is entirely proper. We also note that it can take up to eight weeks or longer from the appointment of an officeholder to having the suppression of their address activated by ASIC and therefore the personal information is made public for up to two months.

Notwithstanding this, while it is possible for an individual to apply to have their address details suppressed on ASIC's register because of safety concerns, the issue we are raising is one that touches every person whose details are on the ASIC register.

Moreover, any legacy system will hold the information of officeholder whose personal details have been registered over many years and in relation to multiple companies. In a world where electronic information remains traceable and accessible, even if no longer posted, such information remains 'live', available and therefore readily accessible, irrespective of an individual's changed status.

Governance Institute is of the view that open publication of birthdates and birth places serves no useful purpose other than for persons with criminal intent. In this world of increasingly faceless transactions, birthdates have unfortunately become by default the first form of identity check by banks, telecommunications companies and other institutions to ascertain that they are communicating with an authorised person. To make readily available the personal information of the business community's most influential officeholders is fraught with risk and a significant magnet for cyber-criminals.

Governance Institute believes that while it is appropriate that ASIC request and retain the personal details of all officeholders on a database subject to strict controls in relation to access, such details should not be available on the public register. One alternative would be to issue an ID number to each officeholder so that any information on them can be retrieved by the regulator as required.

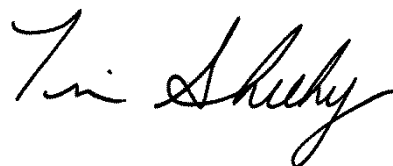
Governance Institute therefore recommends that ASIC retain the personal details of all officeholders but not display the date of birth, residential address and place of birth on the public register.

We also note that the proposed sale of ASIC's registry business highlights further the issues we have raised in this letter. Issues of data control, security and assurance will need to be considered in relation to the sensitive information currently held on the ASIC register.

Should ASIC be of the view that such personal information should continue to be made public, in light of the very real risks that officeholders are exposed to, we recommend that ASIC investigate whether it can immediately implement the address suppression process so that the information is not made public for any period of time.

We would be more than happy to meet with you to discuss this matter.

Yours sincerely

A handwritten signature in black ink, reading "Tim Sheehy". The signature is written in a cursive, flowing style.

Tim Sheehy
Chief Executive

cc Kate O'Rourke, Senior Executive Leader, Corporations, ASIC
Jane Eccleston, Senior Executive Leader, Corporations, ASIC