2018 AUSTRALIAN IPO REVIEW: KEY US SECURITIES DEVELOPMENTS

16 April 2019 | Australia
Legal Briefings – By **Tom O'Neill, Siddhartha Sivaramakrishnan and Laura Sheridan Mouton**

LIQUIDITY TO CONTINUE DESPITE US GOVERNMENT SHUTDOWN

The US capital markets continue to provide a valuable source of funding for Australian companies. Larger Australian IPOs and capital raisings continue to be structured to access US investors and our securities practice has enabled us to act for issuer and underwriter on both the Australian and US law aspects of equity and debt offerings in 2018.

Developments in US federal securities law and regulation and, more generally, the policy direction of US lawmakers and the US Securities and Exchange Commission (the **SEC**) have significant implications for securities offering execution practices around the world, both in the context of IPOs and other offerings registered with the SEC, as well as offerings exempt from SEC registration undertaken pursuant to Rule 144A and as traditional private placements. All of these offering structures are used by Australian issuers.

The past year has seen the SEC continue its efforts to strike a balance between encouraging capital formation and protecting investors:

- the SEC sustained its razor sharp focus on initial coin offerings (**ICOs**) and offerings involving other digital assets in 2018, intensifying its enforcement activity against issuers and other market participants;
- the SEC released interpretive guidance and undertook cybersecurity-related enforcement actions, highlighting its expectation that companies implement appropriate

internal accounting controls to mitigate cyber-related risks and protect company assets in compliance with US federal securities laws; and

- as part of its ongoing disclosure effectiveness initiative, the SEC finalised a series of amendments to disclosure standards that had become redundant, duplicative, overlapping or outdated, and addressed several specific topics where, in its view, disclosure to investors should be improved. Both staff guidance and SEC enforcement activity highlight the SEC's focus on enhancing the utility of corporate disclosures for the investing public – and willingness to take action where company disclosures fail to comply with SEC standards and related staff guidance.

While the SEC has maintained its focus on regulatory compliance and enhancing investor protection, the launch of the SEC's Strategic Hub for Innovation and Financial Technology (**FinHub**) has underscored the SEC's additional commitment to working with fintech developers, entrepreneurs, investors and other market participants on new approaches to capital formation, market structure and financial services. Recognition by SEC staff that digital assets functioning on "sufficiently decentralised" networks may no longer constitute securities for purposes of the US federal securities laws has been welcomed by fintech developers. The roadmap for compliance by unregistered ICOs identified through recent settlement orders is also anticipated to assist entrepreneurs and developers in navigating the regulatory landscape. Further, potential expansion of the "testing the waters" relief (currently available only to emerging growth companies) may also incentivise corporates with significant revenues to undertake SEC registered IPOs and list their equity securities on a US exchange.

INITIAL COIN OFFERINGS REMAIN IN SHARP FOCUS

The SEC continued its razor sharp focus on ICOs and offerings involving cryptocurrencies in 2018, undertaking enforcement action against issuers and various other market participants, both in respect of fraudulent transactions and violations of the registration requirements under the US federal securities laws. In a major speech in June 2018, the Director of the SEC Division of Corporation Finance, William Hinman, articulated the SEC staff's approach to evaluating whether a digital asset constitutes a security.

The SEC has re-emphasised the applicability of the US federal securities laws to virtual organisations and entities that use distributed ledger or blockchain technology to facilitate capital raising and/or investment, and related offers and sales of securities. Amplifying prior guidance – that "by and large" ICOs involve the offer and sale of securities and directly implicate the registration requirement under the US Securities Act (the **Securities Act**) and the anti-fraud provisions of the US federal securities laws – SEC Chairman Jay Clayton confirmed in testimony before the United States Senate in February 2018, "I believe every ICO I've seen is a security".

In particular, the SEC has broadly condemned structuring approaches under which tokens are asserted to provide investors with certain "utility" characteristics as elevating "form over substance". The SEC has explicitly warned that it has not endorsed the approach under the Simple Agreement for Future Tokens (**SAFT**) framework, which seeks to distinguish (i) the initial stage private funding by accredited investors pursuant to the SAFT investment contract (which is acknowledged to be a security), from (ii) the tokens offered to investors once the network is functional (which are asserted under the SAFT framework to not constitute securities).

Director Hinman's June 2018 speech – since endorsed by Chairman Clayton as reflecting the approach taken by the SEC staff in evaluating whether a digital asset is a security – identifies two non-exhaustive sets of factors to be considered in assessing whether a particular digital asset transaction will be subject to the US federal securities laws, each focusing on whether the value received for the digital asset is invested in a common enterprise with a reasonable expectation of profit derived from the efforts of others. Expressly acknowledging that the digital asset itself may not be a security (as is the case for Bitcoin and Ether), Director Hinman highlighted that the primary issue in determining whether a digital asset is offered as an investment contract (and thus constitutes a security) is "whether a third party . . . drives the expectation of a return". When the network on which a digital asset functions becomes sufficiently decentralised that investors do not have an expectation of profits based on the efforts of others (and are purchasing the digital asset for consumption, as compared to investment), the digital asset may no longer constitute a security.

At the time of finalisation of this article, the "plain English" guidance that will assist developers in determining whether their cryptocurrency and token offerings constitute the offer and sale of securities under US federal securities laws (as promised by Director Hinman in November 2018) had not yet been released.

During 2018 the SEC undertook enforcement action against issuers engaged in unregistered ICOs, celebrity promoters of ICOs, an unregistered cryptocurrency exchange, unregistered crypto investment funds and hedge funds and unregistered investment advisers. A November 2018 joint statement by the SEC Division of Corporation Finance, the SEC Division of Investment Management and the SEC Division of Trading and Markets also highlighted the applicability of the US Investment Company Act and the US Investment Advisers Act to investment vehicles engaged in investing in digital assets and their service providers.

However, the launch of the FinHub in October 2018 reflects the SEC's commitment to working with fintech developers, entrepreneurs, investors and other market participants on new approaches to capital formation, market structure and financial services, while maintaining its focus on regulatory compliance and enhancing investor protection. Indeed, November 2018 settlement orders against CarrierEQ Inc. (**AirFox**) and Paragon Coin Inc. (**Paragon**) pave a path to compliance for unregistered ICOs. In addition to imposing civil penalties, these orders required Airfox and Paragon to register their tokens as securities under the US Securities Exchange Act, to file periodic reports with the SEC and to compensate token purchasers. Specifically, Airfox and Paragon were required to notify each token purchaser of its rescission rights (ie to be reimbursed for its original purchase or to sue for recovery or damages if such purchaser no longer owned the tokens). We believe that the compensation and registration requirements included in the AirFox and Paragon settlements are likely to be imposed in future settlements in respect of unregistered ICOs that did not qualify for an exemption from registration. The settlement framework is also instructive for issuers of unregistered ICOs seeking to comply with the US federal securities laws.

OUR TAKE

We expect the SEC to continue to vigorously police the cryptocurrency markets in 2019. In view of the roadmap for remediation of non-compliance provided by the AirFox and Paragon actions, we anticipate that enforcement activity against unregistered ICOs will intensify during the coming year, with the SEC likely to be unsympathetic to issuers whose ICOs failed to qualify for an exemption from Securities Act registration, irrespective of whether some attempts to qualify were made. Recent statements by the SEC and the launch of FinHub reflect the SEC's efforts to encourage technological innovations that benefit investors in the fintech space, while ensuring adherence by all market participants involved in the issuance and trading of digital assets with the requirements of the US federal securities laws.

We envisage that the promised "plain English" guidance will provide market participants with further clarity as to the circumstances under which digital asset transactions constitute an offer and sale of securities under US federal securities laws. We also expect further legislative initiatives in relation to the regulation of digital assets during the coming year. We anticipate that any comprehensive statutory regime will seek to clarify the scope of the regulatory powers of the SEC, the US Commodity Futures Trading Commission, the US Department of the Treasury, the US Federal Reserve and other US federal regulators, and to bridge existing jurisdiction gaps between federal agencies.

CYBERSECURITY CONTINUES TO BE A KEY PRIORITY AREA

Recognising the increasing frequency of cybersecurity-related threats and misconduct, and the heightened impact of cyber violations on investors and the capital markets, the SEC has identified cyber threats as “among the greatest risks facing investors and the securities industry”. During 2018, the SEC released further interpretive guidance to assist companies in preparing disclosure in relation to cybersecurity risks and incidents, and issued a report of investigation highlighting the need for issuers to design and maintain internal accounting control systems that adequately address cybersecurity risks. Following the formation of the Cyber Unit within the SEC Division of Enforcement in late 2017, cybersecurity enforcement activity increased during 2018, with the SEC bringing its first disclosure-based cybersecurity enforcement action, while continuing to focus on cyber-related misconduct used to gain unlawful market advantage and failures by registered entities to take appropriate steps to safeguard information or ensure system integrity.

New interpretive guidance released by the SEC in February 2018 consolidates and builds upon the principles-based guidance issued by the staff of the SEC Division of Corporation Finance in 2011 in relation to cybersecurity disclosure. The 2018 interpretive guidance reinforces cybersecurity considerations relevant to a company’s disclosure of risk factors, operating and financial review and prospects/management’s discussion and analysis of financial condition and results of operations (**MD&A**), business operations, legal proceedings, financial statements, and disclosure controls and procedures. The guidance highlights that disclosures should provide specific information that is useful to investors (rather than generic or boilerplate language) and that, when preparing risk factor disclosure, companies should consider, among other issues:

- the occurrence of prior cybersecurity incidents, including their severity and frequency;
- the probability of the occurrence and potential magnitude of cybersecurity incidents, and the adequacy of preventative actions taken to reduce cybersecurity risks;
- the aspects of the company’s business and operations that give rise to material cybersecurity risks, the costs associated with maintaining cybersecurity protections and the potential for reputational harm; and
- litigation, regulatory investigation and remediation costs associated with cybersecurity incidents.

The 2018 interpretive guidance emphasises that, to meet their disclosure obligations, companies may need to disclose previous cybersecurity incidents or threatened cyber incidents in order to place discussions of these risks in the appropriate context. A company should also address cybersecurity risks and cyber incidents in its MD&A if the costs of cybersecurity efforts, the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend or uncertainty that is reasonably likely to have a material effect on the company's results of operations, liquidity or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition. Further, the 2018 interpretive guidance emphasises the importance of disclosure controls and procedures that enable companies to make accurate and timely disclosures about material cybersecurity incidents, as well as policies that protect against corporate insiders trading in advance of company disclosures of material cybersecurity incidents.

The SEC also initiated its first disclosure-based cybersecurity enforcement action in 2018. In April 2018, Altaba Inc. (formerly, Yahoo! Inc. (**Yahoo**)) agreed to pay US$35 million in penalties for its failure to disclose a data breach in 2014 affecting more than 500 million of its user accounts. Although information relating to the data breach was reported to members of Yahoo's senior management and legal department in late 2014, Yahoo "failed to properly assess the scope, business impact, or legal implications of the breach" and to adequately consider whether the breach needed to be disclosed to investors. Yahoo did not disclose the data breach or its potential business impact and legal implications in its public filings for more than two years. Instead, the company's risk factor disclosures in its SEC filings for the period from 2014 to 2016 were materially misleading in suggesting that Yahoo faced only the risk of, and negative effects that might flow from, potential future data breaches. Moreover, the MD&A disclosure included in these SEC filings was also misleading to the extent that it omitted known trends or uncertainties with regard to liquidity or net revenue presented by current or future expenses or losses related to the 2014 data breach.

Various enforcement and investigative actions initiated by the SEC over the last year have reinforced the importance of comprehensive cybersecurity risk management policies and procedures. The SEC's cease and desist order against Altaba found that the company failed to maintain disclosure controls and procedures designed to ensure that reports from the company's information security team concerning cyber breaches, or the risk of such breaches, were properly and timely assessed for potential disclosure. A September 2018 cease and desist order against broker-dealer Voya Financial Advisers highlights that cybersecurity procedures must be reasonably designed to fit a company's specific business model. The SEC's October 2018 report of investigation – examining whether certain SEC reporting companies that were victims of cyber-related frauds may have violated the US federal securities laws by failing to have sufficient systems of internal accounting controls – further highlighted the need for companies to reassess their controls in view of the current cybersecurity risk environment. In particular, the SEC emphasised the importance of taking into account both cybersecurity threats and related human weaknesses when designing and maintaining internal accounting controls, as well as the critical role of personnel training in implementing controls that serve their purpose and protect company assets in compliance with US federal securities laws. While the SEC concluded that enforcement action was not warranted against the nine SEC reporting companies investigated, the report of investigation serves as a warning that the SEC will proactively scrutinise whether an issuer has implemented appropriate internal accounting controls to mitigate cyber-related risks, and that a company that falls victim to a future data breach or cyber-fraud may be subject to enforcement action as a result of inadequate controls.

OUR TAKE

In view of the Altaba cybersecurity disclosure enforcement action and the warning sounded by the October 2018 SEC report of investigation, we expect the SEC to vigilantly examine companies' cybersecurity disclosures, whether companies' internal accounting controls are adequate to mitigate the risk of cyber-incidents and safeguard company assets, and whether companies' disclosure controls and procedures facilitate timely assessment of appropriate disclosure in relation to cyber breaches and threats. In view of the SEC's focus on this area, we anticipate an increase in enforcement activity in response to cybersecurity incidents, as well as potentially in private litigation related to cyber breaches. We would advise issuers:

• to ensure that their cybersecurity disclosure is tailored to their specific business and operations, and industry context;

• to consider whether their insider trading policies protect against corporate insiders trading in advance of company disclosures of material cybersecurity incidents;

• to reassess their cybersecurity risk management policies and procedures in light of emerging cyber-related risks and threats, to implement internal controls tailored to address cybersecurity risks relevant to their particular business and operations, and to prioritise the training of employees on those policies and procedures; and

• to involve outside advisors early in the process when analysing and responding to any cybersecurity incident.

CONTINUED FOCUS ON MATERIAL INFORMATION DISCLOSURES

Continuing its focus on improving disclosure effectiveness, in August 2018 the SEC adopted a series of amendments to disclosure standards that had become redundant, duplicative, overlapping or outdated in light of other SEC disclosure requirements, US GAAP, International Financial Reporting Standards or changes in the information environment. The final rules, which largely enact the proposals released by the SEC in July 2016, eliminate requirements to provide business disclosure in relation to segment financial information, research and development expenditures and financial information by geographic area. The amendments also update certain disclosure standards in relation to market information, trading prices for equity securities and dividend history.

At the time of finalising this article, the SEC's October 2017 proposals to modernise and simplify disclosure standards under Regulation S-K (and corresponding requirements applicable to non-US issuers, as set out in Form 20-F) remain pending. These proposed rules would, among other things:

- revise MD&A disclosure requirements – in certain circumstances, permitting an issuer to omit discussion of the earliest year of the three year period covered by the financial statements if such disclosure is not material to an understanding of the company's financial condition, changes in financial condition and results of operations – with the intent of encouraging companies to take a "fresh look" to re-evaluate whether prior year MD&A disclosures remain material;
- eliminate risk factor examples currently enumerated in Regulation S-K, to encourage issuers to focus on their own risk identification processes;
- remove certain restrictions on incorporation by reference; and
- permit the omission of certain immaterial, competitively sensitive information that has not been made public.

Rule amendments proposed in July 2018 that would simplify financial disclosure requirements in respect of guarantors and issuers of guaranteed securities, as well for affiliates whose securities collateralise an issuer's securities, also remain pending at the time of finalising this article.

In furtherance of its disclosure effectiveness reform agenda, in October 2018, the SEC adopted final rules modernising industry-specific disclosure requirements applicable to companies with mining operations that are material to their business or financial condition. Replacing SEC Industry Guide 7 (which, prior to the reforms, had not been updated in over 30 years), the final rules more closely align US disclosure requirements with current industry and global regulatory practices and standards, including the mining disclosure standards based on the Committee for Mineral Reserves International Reporting Standards. For each fiscal year beginning on or after 1 January 2021, SEC registrants with material mining operations will be required to disclose (i) mineral resources (disclosure of which was generally prohibited under previous SEC disclosure standards, which did not provide for the reporting of estimates other than proven reserves (ie measured mineral resources) or probable reserves (ie indicated mineral resources)), (ii) mineral reserves and (iii) material exploration results, as confirmed by a relevant mining industry professional providing a technical report. Closer alignment of the SEC's mining property disclosure requirements with the Australasian Code for Reporting of Exploration Results, Mineral Resources and Ore Reserves (the **JORC Code**) and other foreign mining codes is anticipated to facilitate access to US capital markets.

In a November 2018 speech, Chairman Clayton further reinforced that companies should tailor their disclosures in relation to market risks – in particular, in respect of Brexit and the transition away from LIBOR as a benchmark reference for financial contracts – and review and revise their disclosures on an ongoing basis to ensure that they accurately and specifically disclose the key risks that a company may face as a result of Brexit and/or the transition from inter-bank offered rates to alternative measures. Specifically, Chairman Clayton has confirmed that he would like to see "robust disclosure on how management is considering Brexit and the impact it may have on the company and its operations". Similarly, companies with significant exposure to instruments based on LIBOR (or other reference rates) should consider disclosing (i) what happens to the interest rates due under the instrument if LIBOR (or such other reference rate) is no longer published, (ii) whether the instrument includes any "fall-back" language for the determination of interest rates following LIBOR phase-out after 2021 and, if so, how such language would work in practice and (iii) whether consents would be required to amend the terms of the instrument and, if so, whether there are risks that such consents would not be able to be obtained in a timely or cost-effective manner.

Recent enforcement activity also confirms the SEC's focus on enhancing the utility of corporate disclosures for the investing public, including through the vigilant monitoring of company disclosures for compliance with SEC standards and related staff guidance. Reflecting the SEC Division of Corporation Finance's efforts to curb non-compliant use of non-GAAP financial measures, in December 2018 the SEC ordered an SEC registrant to pay civil penalties and to cease and desist from further violations of Regulation S-K's "equal or greater prominence" standard, which requires a company disclosing a non-GAAP financial measure to include a presentation, with "equal or greater prominence", of the most directly comparable financial measure calculated and presented in accordance with generally accepted accounting principles. Further, recent investigations and enforcement actions by the SEC in relation to executive compensation disclosures (particularly in view of its December 2018 adoption of disclosure rules for hedging practices and policies with respect to equity securities) similarly highlight the SEC's focus on ensuring that investors have access to material information – and its willingness to initiate enforcement activity where company disclosures fail to comply with SEC disclosure standards.

OUR TAKE

Reforms proposed and adopted by the SEC in 2018 continue to modernise the disclosure framework, consistent with the SEC's disclosure effectiveness initiative – which we have previously described as "evolution, not revolution". With the SEC focused on enhancing the readability and navigability of disclosure documents, discouraging repetition and the disclosure of immaterial information, and reducing the cost and burden of compliance, we anticipate that a form of the Regulation S-K reforms proposed in October 2017 will be adopted during the course of 2019. Following its adoption of revised disclosure requirements for SEC registrants engaged in mining in October 2018, we also expect the SEC to progress its reform of the industry-specific disclosure requirements applicable to bank holding companies (as currently reflected in SEC Industry Guide 3) during the course of 2019.

The SEC's willingness to engage in modernisation and enhancement of the disclosure framework while also addressing, through formal and informal guidance, particular disclosure topics that it believes will materially impact investors is a helpful approach for investors and promotes the efficiency of the securities markets and capital formation.

PROPOSED EXTENSION OF "TESTING THE WATERS" PROVISIONS"

In February 2019, the SEC proposed amendments to extend the "testing the waters" procedures adopted pursuant to the Jumpstart Our Business Startups Act (**JOBS Act**) enacted in 2012 to non-emerging growth companies. Under the JOBS Act, emerging growth companies (ie companies with annual gross revenues of less than US$1.07 billion during the most recently completed fiscal year) and persons authorised to act on their behalf may "engage in oral or written communications with potential investors...to determine whether such investors might have an interest in a contemplated securities offering, either prior to or following" the filing of a registration statement under the Securities Act. Pre-filing communications are limited to investors that are qualified institutional buyers pursuant to Rule 144A under the Securities Act or institutional accredited investors pursuant to Regulation D under the Securities Act.

Under the current statutory regime, companies that do not constitute emerging growth companies are not permitted to utilise the "testing the waters" procedures – and are consequently unable to assess investor interest in a potential IPO before incurring the substantial costs associated with preparing a registration statement. Consistent with its commitment to facilitating capital formation and in an effort to encourage more companies to go through the US IPO process; the proposed expanded "testing the waters" provision would provide non-emerging growth companies with increased flexibility in their pre-IPO communications, as well as a cost-effective means of evaluating market interest before determining to proceed with an IPO.

OUR TAKE
While the majority of IPOs by Australian issuers that are directed to the US capital markets are structured to be exempt from SEC registration, US listings offer particular attractions for sector-specific and significantly-sized Australian issuers. An extension of the "testing the waters" provision to larger companies would enable more Australian companies to assess investor interest – and potential valuation – prior to undertaking preparations for a US IPO. We believe that the availability of this relief will incentivise more companies with significant revenues to consider SEC registered IPOs and listing of their equity securities on a US exchange.

REVIEW OF THE PRIVATE OFFERING FRAMEWORK

In August 2018, Chairman Clayton indicated that the SEC intends to evaluate the level of complexity of the current framework of private offering exemptions, and consider whether changes should be made to rationalise and streamline what he described as an"elaborate patchwork" of regulation.

The SEC plans to consider:

- whether there are currently overlapping private offering exemptions that create confusion for companies trying to navigate the most efficient path to raise capital;
- whether the current rules that limit who can invest in certain offerings should be expanded to focus on the sophistication of the investor, the amount of the investment, or other criteria rather than just the wealth of the investor; and
- if more can be done to allow issuers to transition from one exemption to another and, ultimately, to a registered IPO, without undue friction.

The SEC staff is currently working on a concept release that will bring to the forefront these and other topics relevant to this issue. The SEC is hoping for significant input from companies, banks and investors on the concept release.

OUR TAKE
Given the frequent use by non-US issuers (including Australian issuers) of the private offering exemptions under Section 4(a)(2) of the Securities Act and pursuant to Rule 144A (when raising capital from large institutional investors in the United States), the concept release is likely to be important reading for Australian issuers and financial intermediaries.
Once the concept release has been issued, Herbert Smith Freehills will circulate a client memorandum on the implications of the review for non-US issuers looking to access the US capital markets. There will also be a public comment period and we expect to submit a comment letter to the SEC. We would welcome your views as part of this process.

Please click here to return to the main page

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

TOM O'NEILL
PARTNER, HEAD OF US SECURITIES, LONDON
+44 20 7466 2466
Tom.ONeill@hsf.com

LEGAL NOTICE