SEC CHAIRMAN COMMENTS ON BREXIT, LIBOR AND CYBERSECURITY RISKS

03 January 2019 | Global
Legal Briefings – By **Tom O'Neill, Dinesh Banani, Dennis Hermreck and Juan Grana**

On 6 December 2018, the Chairman of the US Securities and Exchange Commission (the "**SEC**"), Jay Clayton, delivered a speech[1] in New York where he identified the United Kingdom's exit from the European Union ("**Brexit**"), the transition away from LIBOR and cybersecurity as key market risks that the SEC is closely monitoring in its review of US public company disclosures.

Although Chairman Clayton's remarks were directed towards SEC reporting companies, the market risks he highlighted should also be considered by foreign private issuers with securities listed in other jurisdictions (particularly the United Kingdom and Europe) as they prepare their public company disclosure (including annual reports) and securities offering documentation, particularly when such documentation is being prepared to a Rule 144A standard. In view of the rapidly changing environment, particularly with respect to Brexit, we would also recommend that companies revisit their disclosure as necessary to ensure it continues to be responsive to material changes in circumstances.

BREXIT

In his remarks, Chairman Clayton expressed concern that:

> the potential adverse effects of Brexit are not well understood and, in the areas where they are understood, may be underestimated by issuers;

> the actual effects of Brexit (a) will depend on many factors, some of which may prove beyond the control of UK and EU authorities; (b) are likely to manifest themselves in advance of implementation dates and some of those effects are already upon us; and (c) will depend in large part on the ability of UK and EU officials to provide a path forward that allows for adjustment without undue uncertainty, disruption or cost, which may be a tall order as it requires a broad understanding of market interdependencies and considerable foresight and flexibility; and
>
> limiting the adverse effects of Brexit will require a willingness of governmental authorities to look beyond potential immediate, local economic and other opportunities provided by a blunt transition so as to pursue a course that focuses on broad, long-term economic performance and stability, which may be difficult to achieve in practice.

As a result, Chairman Clayton has directed the SEC staff to focus on the disclosures companies make about Brexit and, going forward, would like to see issuers provide more robust disclosure about how management is considering Brexit and the potential impact Brexit may have on a company and its operations.

Chairman Clayton also noted that the SEC commenced discussions with its UK and EU counterparts and with market participants regarding Brexit-related impacts on investors and markets following the 2016 Brexit referendum and that he expects the pace of these discussions to now increase.

Given the fast moving nature of the current Brexit discussions, issuers will need to review their Brexit-related disclosures on an ongoing basis to ensure that they have accurately and specifically disclosed the key risks that a company may face as a result of Brexit.

LIBOR

The second key market risk highlighted by Chairman Clayton's speech is the transition away from LIBOR as a reference rate for financial contracts. LIBOR is used extensively in the US and globally as a benchmark for various commercial and financial contracts, including interest rate swaps and other derivatives, as well as floating rate mortgages and corporate debt. The banks currently reporting information used to set LIBOR may stop doing so after 2021, when their commitment to report information used to set LIBOR ends.

The US Federal Reserve estimates that in the cash and derivatives markets there are approximately $200 trillion in notional transactions referencing US Dollar LIBOR and that more than $35 trillion of these will not mature by the end of 2021. The Alternative Reference Rate Committee (the "**Committee**"), a committee convened by the US Federal Reserve that includes major market participants, and on which the SEC staff and other regulators participate, has proposed an alternative rate to replace US Dollar LIBOR—the Secured Overnight Financing Rate ("**SOFR**").

The Committee has identified certain benefits to using SOFR as an alternative to LIBOR. For example, SOFR is based on direct observable transactions and on a market with very deep liquidity, reflecting overnight US Treasury repurchase agreement transactions with daily volumes regularly in excess of $700 billion.

However, a significant risk for many market participants is how to manage the transition from LIBOR to a new rate such as SOFR, particularly with respect to instruments based on LIBOR that will still be outstanding at the end of 2021. Accordingly, companies with significant exposure to instruments based on LIBOR should consider disclosing, for example:

- what happens to the interest rates due under the instrument if LIBOR stops being published;
- whether there is any "fall-back" language for the determination of interest rates under the instrument and, if so, how such language would work in practice; and
- whether consents will be needed to amend 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.

CYBERSECURITY

Chairman Clayton also highlighted that the SEC is focussing on the disclosure of cybersecurity risks and incidents and drew attention specifically to recent SEC guidance regarding cybersecurity disclosures.[2] Under the guidance, companies are required to disclose cybersecurity risks and incidents where they are material and such disclosures should provide specific information that is useful to investors (while avoiding generic or boilerplate language). For example, when preparing risk factor disclosure, companies should consider:

- the occurrence of prior cybersecurity incidents, including their severity and frequency;
- the probability of the occurrence and potential magnitude of cybersecurity incidents;

the adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs, including, if appropriate, discussing the limits of the company's ability to prevent or mitigate certain cybersecurity risks;

the aspects of the company's business and operations that give rise to material cybersecurity risks and the potential costs and consequences of such risks, including industry-specific risks and third-party supplier and service provider risks;

the costs associated with maintaining cybersecurity protections, including, if applicable, insurance coverage relating to cybersecurity incidents or payments to service providers;

the potential for reputational harm;

existing or pending laws and regulations that may affect the requirements to which companies are subject relating to cybersecurity and the associated costs to companies; and

litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents.

The guidance emphasised that, in order to meet their disclosure obligations, companies may need to disclose previous cybersecurity incidents in order to place discussions of these risks in the appropriate context. For example, if a company previously experienced a material cybersecurity incident involving denial-of-service, it likely would not be sufficient for the company to disclose that there is a risk that a denial-of-service incident may occur. Instead, the company may need to discuss the occurrence of that cybersecurity incident and its consequences as part of a broader discussion of the types of potential cybersecurity incidents that pose particular risks to the company's business and operations.

The guidance also emphasised 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.

We would be pleased to speak to issuers, other selling security holders or their investment banking advisors with respect to any of these topics.

1. See https://www.sec.gov/news/speech/speech-clayton-120618.

2. See Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166 (Feb.26, 2018).

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

DINESH BANANI
PARTNER, LONDON
+44 20 7466 2042
Dinesh.Banani@hsf.com

DENNIS HERMRECK
COUNSEL (US), LONDON
+44 20 7466 2909
Dennis.Hermreck@hsf.com

LEGAL NOTICE