Key Takeaways

Key Takeaways

Rule	What Companies Should Do Now
Dodd-Frank Clawback Rule	• Adopt new clawback policy and consider any amendments to existing policies • Determine scope of “executive officers” • Consider home country law implications
Amended Rule 10b5-1 and Insider Trading Policy Disclosure	• Ensure that insider trading policies and procedures more broadly are ready for public scrutiny to the extent they had not been previously publicized • Review and, as needed, revise Rule 10b5-1 plan policies for compliance with new rules • Consider interaction with compensatory equity plans and use of sell-to-cover plans • Determine scope of “officers” implicated

Stock Buyback Disclosures	• Disclosure Preparation and Controls
	  • Establish process for collecting data about daily repurchase activity from brokers and repurchase counterparties
	  • Prepare narrative disclosures about purposes and policies for review by management and ensure periodic review and refresh for continued accuracy and completeness
	  • Keep track of adoption/modification/termination of company Rule 10b5-1 plans and collect relevant information for disclosure
	• Policies
	  • Consider restricting trading by D&Os around announcement of repurchase programs or program increases to avoid having to check the box for such trading
	  • Consider policies for trading by D&Os during pendency of repurchase programs
	• Investor Relations
	  • Be prepared for questions from investors and analysts about disclosed changes in daily repurchase activity (consider adopting “no comment” policy)

Key Takeaways (cont.)

Proposed Rule	What Companies Should Do Now

Cybersecurity Disclosure Rules	• Prepare for incident reporting (Form 6-K incident disclosure is triggered only if required under home country or stock exchange rules or otherwise voluntarily reported publicly)
	  • Incident response plans.
	  • Update cybersecurity incident response plans to incorporate new reporting requirements and clearly delineate how, when and who is responsible for determining whether an incident is material and whether disclosure is required or should otherwise be voluntarily reported.
	  • Disclosure controls.
	  • Ensure disclosure committee (or those responsible for making materiality and disclosure decisions) is directly connected to those responsible for evaluating and reporting of the occurrence of a cybersecurity incident.
	  • Review escalation procedures within information security teams that relate to identifying when cybersecurity incidents occur.
	  • After the occurrence of a cybersecurity incident, lines of communication should be enhanced to ensure more frequent updating of appropriate individuals and a reassessment of the status, scope and severity of an incident so that timely materiality assessments can be made as new information becomes available and that any updating disclosures are made in a timely manner.
	  • Effect of public disclosure.
	  • Be mindful that SEC disclosure obligations operate independently of any other provisions of law (such as state or local data protection laws) that may permit or mandate a delay in notifying the public about material cybersecurity incidents.
	  • Consider how the timing of potential disclosures may impact, and potentially accelerate, existing regulatory or contractual obligations.
	  • Assessment must include third-party providers.
	  • Ensure that any information received about third-party incidents is directed into the company's own materiality determination and disclosure process in same manner as incidents involving the company's own systems.

Key Takeaways (cont.)

Proposed Rule	What Companies Should Do Now

Cybersecurity Disclosure Rules (cont.)	• Tracking minor cybersecurity incidents for potential aggregation.
	  • Track minor cybersecurity incidents so an assessment can be made as to whether they are "related" under relevant SEC guidance and therefore need to be aggregated in the company's materiality determination with a view to potential public disclosure.
	• Review cybersecurity risk management and governance.
	  • The new disclosure requirements will likely result in companies describing robust cybersecurity risk identification, assessment and management processes and governance, including an appropriate level of board engagement on cybersecurity matters.
	  • Review and, if needed, enhance existing practices and policies with a view to their public disclosure.
	  • Consider which practices should now be documented to provide the appropriate compliance rigor and to demonstrate the formalization of these processes within the organization.

Climate-Related Disclosure Framework	• Evaluate gaps in current climate-related disclosures • Evaluate the board's oversight of climate risks • Evaluate the process used by management to assess climate risks • Review climate-related goals • Plan for systems required for financial reporting

SHEARMAN & STERLING

ABU DHABI • AUSTIN • BEIJING • BRUSSELS • DALLAS • DUBAI • FRANKFURT • HONG KONG • HOUSTON • LONDON • MENLO PARK • MILAN
NEW YORK • PARIS • RIYADH* • ROME • SAN FRANCISCO • SÃO PAOLO • SEOUL • SHANGHAI • SINGAPORE • TOKYO • TORONTO • WASHINGTON, DC