THOMSON REUTERS
CHECKPOINT™

S. Davis & Associates, P.A.
Certified Public Accountants & Consultants

THE PPC
ACCOUNTING AND AUDITING UPDATE

MARCH 2021, VOLUME 30, NO. 3

COVID-19 Effects on Cash Flow Hedge Accounting

The FASB Staff developed a couple of questions and answers (Q&As) to respond to questions about how to deal with the effects of COVID-19 on cash flow hedge accounting under FASB ASC 815, *Derivatives and Hedging*. The pandemic has caused forecasted transactions to be postponed or cancelled, which can have accounting implications for cash flow hedge accounting under this guidance.

Following is a summary of the Staff's Q&As.

Delays in the Timing of Forecasted Transactions

Q: FASB ASC 815-30-40-4 indicates if cash flow hedge accounting is discontinued, deferred amounts in AOCI should remain unless it's probable the forecasted transaction won't occur by the end of the originally specified time period or within two months thereafter. There is an exception when extenuating circumstances exist related to the nature of the forecasted transaction and outside the influence or control of the entity that may cause the forecasted transaction to be probable of occurring beyond the two-month period. In those rare cases, amounts would continue to be deferred in AOCI until the forecasted transaction affects earnings.

When cash flow hedge accounting has been discontinued, may delays in the timing of the forecasted transactions related to the effects of the COVID-19 pandemic be considered rare cases caused by extenuating circumstances outside the entity's control or influence?

A: The exception in FASB ASC 815 may be applied to delays in timing of forecasted transactions if the delays are related to effects of the COVID-19 pandemic and the forecasted transaction remains probable of occurring. The determination requires judgment based on the facts and circumstances.

If the forecasted transaction is no longer probable of occurring within a reasonable period of time beyond the additional two months because of disruptions to the business related to effects of COVID-19, the exception doesn't apply and amounts

In this Issue:

This newsletter is also available online.
Please call (800) 431-9025, or order online:
https://tax.thomsonreuters.com/products/brands/checkpoint/ppc/

THOMSON REUTERS™

in AOCI should be reclassified to earnings immediately and disclosed in interim and annual financial statements.

Entity's Ability to Accurately Predict Forecasted Transactions

Q: FASB ASC 815-30-40-5 states a pattern of determining that forecasted transactions are probable of not occurring calls into question the entity's ability to accurately predict forecasted transactions and the appropriateness of using cash flow hedge accounting in the future for similar transactions.

If amounts deferred in AOCI should be reclassified to earnings because of missed forecasts related to the effects of the COVID-19 pandemic, should those missed forecasts be considered when determining whether the entity has exhibited a pattern of missing forecasts that would call into question its ability to accurately predict forecasted transactions and the propriety of using cash flow hedge accounting in the future for similar transactions?

A: It's acceptable not to consider missed forecasts related to the effects of COVID-19 when determining whether there has been a pattern of missing forecasts. FASB ASC 815 didn't contemplate forecasts changing so rapidly because of a pandemic. Determining whether the missed forecast is due to the pandemic requires judgment based on facts and circumstances.

If the missed forecast is related to the pandemic, the missed forecast would continue to be accounted for under FASB ASC 815 with appropriate disclosures of the associated amounts.

Practical Consideration:

The FASB Staff Q&A is available on the FASB's website at **www.fasb.org/jsp/FASB/Document_C/DocumentPage&cid=1176174564157**.

FASB Clarifies Reference Rate Reform Guidance

FASB issued ASU 2021-01, *Reference Rate Reform (Topic 848) Scope*, in January 2021. It broadens and clarifies guidance in ASU 2020-04, which was issued in response to changes in global markets resulting from reference rate reform. ASU 2021-01 refers to the market-wide transition to new reference rates as the "discounting transition." It addresses stakeholder concerns about accounting consequences of the transition and is intended to reduce diversity in practice.

ASU 2020-04, *Reference Rate Reform (Topic 848)*, was issued in March 2020, and provided optional alternatives and practical expedients to GAAP for a limited time (through December 31, 2022) to simplify accounting for contracts and hedging relationships affected by reference rate reform. ASU 2020-04 was worded to apply only to transactions that reference LIBOR or another discontinued interest rate. Some questioned whether ASU 2020-04 could also be applied to derivative instruments that don't reference a rate that isn't be discontinued but use an interest rate for margining, discounting, or contract price alignment that is modified due to reference rate reform.

ASU 2021-01 expanded the scope of ASU 2020-04 to clarify that all derivatives whose interest rates are modified by the discounting transition, so they are eligible for the expedients.

Following is a summary of some of the other main points of ASU 2021-01:

- The amendments apply to all entities with derivatives that use an interest rate being modified because of the discounting transition. Entities that designate certain interest rate swaps as hedging instruments in net investment hedges being modified due to the reform can also optionally apply the guidance.
- FASB ASC 848 has subtopics with optional exceptions and expedients related to contract modifications and hedge accounting that can be elected and applied to contracts and derivatives that use an interest rate affected by the discounting transition.
- Receive-variable-rate, pay-variable-rate cross currency interest rate swaps may be considered eligible hedging instruments in a net investment hedge if both legs of the swap don't have the same repricing intervals and dates as a result of reference rate reform.

ASU 2021-01 is effective immediately. It can be applied retrospectively as of any date beginning with an interim period that includes or is subsequent to March 12, 2020, or prospectively to new modifications made from any date within an interim period that includes January 7, 2021 (the date the ASU was issued), up to the date the financial statements are available to be issued.

If ASU 2021-01 is applied to an eligible hedge, adjustments resulting from the election must be recorded as of the date the election is applied.

Consistent with ASU 2020-04, ASU 2021-01 doesn't apply to contract modifications made after, or new hedges entered into after, December 31, 2022. It also doesn't apply to existing hedges evaluated for effectiveness after December 31, 2022, unless the hedges existed as of December 31, 2022 and the optional expedients are applied and the accounting effects are recorded through the end of the hedge relationship (including periods after December 31, 2022).

Companies electing to apply the optional expedients in FASB ASC 848 may need to update their hedge accounting documentation. They should also consider the need to disclose the impacts of the ASU, including the reason for adopting the relief provisions.

• • •

Cybersecurity: Risks and Opportunities

Cybersecurity threats and security breaches are too frequently in the headlines. As businesses increasingly rely on technology, markets for products and services have gone global, cyber threats are more sophisticated and aggressive, and risks are increasing. Cybersecurity threats pose risks to CPA firms themselves and to their clients. The cybersecurity threats posed to clients provide client service opportunities for CPA firms.

The AICPA's PCPS, in conjunction with LBMC, developed a tool, *A CPA's Introduction to Cybersecurity*, that summarizes the risks to firms and their clients and the policies and practices that should be put in place to mitigate these risks. Here are highlights of that tool:

- *Cybersecurity* is a process where controls are designed and implemented to identify potential threats, protect systems and information from security events, and detect and respond to breaches that occur.
- *CPA firms are at risk* for cyberattacks because they are a single access point for data from a number of clients. They also have client data stored in many places (laptops, firm networks, cloud-based storage, email, portals, mobile devices, flash drives), so there are many potential areas for unauthorized access. Firms handle sensitive data, including personally identifiable information (PII), protected health information (PHI), and payment card industry (PCI) data, and they must have effective controls to manage their compliance obligations under federal and state laws and industry standards.
- *Clients are at risk* for many of the same reasons as CPA firms. Smaller companies may not have the resources to support a cybersecurity program, but a security breach to a company of any size can cause loss of customers, reputational damage, and even cause them to go out of business. CPA firms can help clients understand and manage cybersecurity risks because they understand their clients' businesses, are specialists in risk assessment and implementation of internal controls, and regularly handle clients' sensitive information and can make recommendations about controls over data security.
- *Cybersecurity policies and practices* every CPA firm should consider for themselves, and potentially recommend to their clients, include: (1) an overall risk assessment and periodic reassessment of security measures; (2) identification of sensitive data and where it is held; (3) requiring that passwords be strong and protected, keeping operating software updated and secure; (4) having a security monitoring and alert system in house or outsourced to specialists; and (5) developing backups and a continuity plan. Employees should be trained on IT security policies, the number of IT administrators should be limited, and outside parties that support the CPA firm should be held responsible for cybersecurity through contracts and annual compliance reporting.

Firms need an incident response plan that includes recovering from an event and communicating with all affected parties.

Practical Consideration:

The AIPCA's tool, *A CPA's Introduction to Cybersecurity*, is available to AICPA members at **www.aicpa.org/InterestAreas/PrivateCompaniesPracticeSection/QualityServicesDelivery/InformationTechnology/DownloadableDocuments/cpa-guide-to-cybersecurity.pdf?utm_source=mnl:cpald**.

The AICPA's Assurance Services Executive Committee released for public comment two sets of criteria on cybersecurity. One is for management's use in designing and describing its cybersecurity risk management program and for accounting firms to report on it. The other is for public accounting firms that provide advisory or attest services on an entity's controls over cybersecurity risk management. The AICPA hopes to develop a new cybersecurity risk management framework with common criteria that will lay the groundwork for CPAs

The PPC Accounting and Auditing Update is published monthly by Thomson Reuters/Tax & Accounting, P.O. Box 115008, Carrollton, Texas 75011-5008, (800) 431-9025.

THOMSON REUTERS™

Tax & Accounting - Checkpoint
P.O. Box 115008
Carrollton, Texas 75011-5008
UNITED STATES OF AMERICA

ADDRESS SERVICE REQUESTED

PRSRT STD
U.S. POSTAGE
PAID
Thomson

to provide new assurance services on the effectiveness of an entity's cybersecurity risk management program (a cybersecurity examination).

Practical Consideration:

Information about this initiative and other AICPA resources relating to cybersecurity are available on the AICPA's website at **www.aicpa.org/interestareas/frc/assuranceadvisoryservices/cybersecurity-resource-center.html**.

The Securities and Exchange Commission (SEC) has also made cybersecurity a priority. It is providing guidance to help investors protect themselves, along with information for broker-dealers, investment advisors, stock exchanges, and other market participants. Their Division of Enforcement established a Cyber Unit in 2017 to focus on violations and cybersecurity controls. The SEC's activities and resources on cybersecurity can be useful to management and accountants of both public and private companies.

Practical Consideration:

SEC resources on cybersecurity are available on the SEC's website at **www.sec.gov/spotlight/cybersecurity**.