FINANCIAL SERVICES BOARD INSIGHTS

Tax Reform Update: One Big Beautiful Bill Act

With the recent signing of Public Law No. 119-21 — aka the One Big Beautiful Bill (OBBB) — a number of provisions from the 2017 Tax Cuts and Jobs Act (TCJA) that were set to change or sunset at the end of 2025, were extended. Here's an overview of several topics of interest to bank leadership.

Business Tax Reforms

- Exclusion of 25 percent of interest received by a qualified lender on any qualified real estate loan effective for original debt incurred in tax years ending after July 4, 2025.
- Restoration of 100 percent bonus depreciation in the year the asset is placed into service for most business assets placed into service after Jan. 19, 2025, replacing the phased-down depreciation that began in 2023.
- Reforms to low-income housing tax credits (LIHTC) make it easier for more projects to qualify for the 4 percent tax credit and make permanent a 12 percent annual increase for certain LIHTC allocations.
- Corporations may only deduct charitable contributions that exceed 1 percent of the corporation's taxable income, up to a cap of 10 percent of taxable income. Contributions above 10 percent of taxable income may be carried forward for five years.
- Beginning Jan. 1, 2026, employers will no longer be able to deduct certain meal-related expenses, such as snacks, coffee, and meals provided on business premises for the convenience of the employer.

CFPB (Consumer Financial Protection Bureau)

In line with the Trump Administration's overall stance on regulation, OBBBA reduces the amount of funding the CFPB can request from the Federal Reserve from 12 percent to 6.5 percent. For FY2025, the funding cap is estimated to be $446 million — 46 percent less than the $823 million it would have been under the 2010 Dodd-Frank Act's formula. While this might limit CFPB rulemaking and enforcement activities, state regulator efforts and private litigation could close any gaps.

Student Loan Programs

OBBBA ends the Graduate PLUS Loan program but introduces the Parent PLUS Loan program, as well as annual and aggregate borrowing limits. These changes may push borrowers to seek alternative, potentially higher-cost financing options. It also moves borrowers into income-based repayment plans and sets stricter eligibility and accounting standards for educational institutions.

Agriculture and Farming

Significant changes to U.S. agricultural industry policy include raising key crop reference prices and enhancing safety net programs. Other changes include the allocation of 30 million new base acres, allowing more farmers to qualify for federal support; increases in payment limits for commodity programs; more financial assistance for dairy farmers; and enhanced premium support for crop insurance.

Trump Accounts

These new tax-advantage savings accounts for eligible minors are capped at $5,000 in contributions annually and feature strict investment and distribution requirements. Children born between Jan. 1, 2025 and Dec. 31, 2028, will each receive an initial $1,000 contribution to their Trump Account from the federal government.

For guidance navigating these and other reforms that will impact your financial institution, as well your personal and business clients, please contact Lisa M. Newland, CPA, CFE, at 239.992.6211 or lisa.newland@rehmann.com.

Mitigating Payment Fraud with Third-party Oversight and Strong Internal Controls

Payment fraud and scams continue to capture the attention of federal regulators due to the risks arising from non-compliance related to third-party service provider (TPSP) failures and inadequate Bank Secrecy Act/Anti-Money Laundering (BSA/AML) programs. In June 2025, the agencies requested comments on potential areas for improvement and collaboration between financial institutions, consumers, and payment processors.

Threats are plentiful and varied. Bad actors use social engineering, phishing, business email compromise, romance and investment scams, and identity theft to target checks, wire transfers, and peer-to-peer payments. TPSPs may become victims of these schemes as well as experience service failures, outages, or data breaches that compromise customer information, impact your ability to process payments, and damage your marketplace reputation. Hackers gain unauthorized access to steal account and credit and debit card numbers. Tactics such as DDoS attacks, malware, and ransomware compromise networks. Employees and contractors may unknowingly or intentionally share sensitive information.

Moreover, the OCC Spring 2025 Semi Annual Risk Assessment noted that gaps in BSA/AML programs, and partnerships with fintechs lacking experience and technical expertise may also elevate payment fraud risks and raise Suspicious Activity Report (SAR) and Currency Transaction Report (CTR) filing obligations. BSA/AML compliance failure scenarios often include weak internal controls and monitoring systems; deficient independent audits; BSA or compliance officers who lack experience, authority or independence; outdated Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD); poor quality transaction monitoring data; overreliance on legacy systems; and insufficient financial resources.

Coupled with the March 2025 U.S. Treasury Department interim final rule removing the requirement to report beneficial ownership to the Financial Crimes Enforcement Network (FinCEN) and the potential for lax compliance with Reg E, Reg CC, and the Federal Trade Commission Act, banks can find it challenging to manage their payment fraud and BSA/AML risk profiles.

These examples emphasize the importance of strong internal controls and programs, coupled with robust TPSP risk management protocols to limit exposure to audit scrutiny, fines, and legal action. Board members should ensure such programs go beyond encryption, tokenization, and secure data storage, and seek a TPSP Service Level Agreement (SLA) that meets these best practices:

- Real-time fraud detection, machine learning, and multi-factor authentication (MFA) to prevent unauthorized transactions
- Uptime guarantees and disaster recovery plans for outages or other disruptions
- Corporate culture that prioritizes employee education and training
- Compliance with Payment Card Industry Data Security Standards (PCI DSS), General Data Protection Regulation (GDPR), and California Consumer Privacy Act (CCPA)
- Defined routines to update systems and data handling processes to keep pace with regulatory changes and ensure data security and integrity

While the Board may delegate daily operational management to others, it is responsible for oversight to ensure the bank operates in a safe and sound manner, consistent with strategic goals, and in compliance with applicable laws and regulations.

We provide expert guidance on executing effective risk management practices that include oversight of TPSPs and BSA/AML programs. Contact Beth Behrend, CCBCO, CBAP at 616.975.4100 or beth.behrend@rehmann.com or Mynesha Phifer at 734.302.4152 or mynesha.phifer@rehmann.com.

Audit Committee Guidelines for AI Oversight

AI technologies are redefining business strategies, employee roles, and workflows as agile companies leverage AI technologies to empower teams and drive innovation. Two common types of AI are: machine learning (ML), feeding large amounts of data into algorithms that analyze and learn from it to predict future outcomes such as economic forecasts and credit risks; and Generative AI (GenAI) which goes beyond analyzing data to create new content that mimics human creations, such as engaging chatbot customer service interactions and the possibility of deepfake audio and video that look "real".

That's why AI impact on products, services, and financial performance must be balanced with proactive risk management, and appropriate processes and controls for oversight of both AI and human-directed activities.

Underscoring AI's impact on financial performance, PricewaterhouseCoopers' Annual CEO Survey, released in January 2025, reported that one-third of CEOs believe AI has increased revenue and profitability over the past year, and one-half expect it to drive increases in profits in the year ahead. In a separate survey of corporate directors, 57 percent said the full board has primary oversight of AI and other emerging technologies, while 17 percent assigned that responsibility to the Audit Committee.

Clearly, the expectation is that the board at large, and Audit Committee members specifically, are responsible for oversight of management's application of AI technologies, including:

- Monitoring the use of AI in financial reporting beyond simply preparing the report to include processes and controls to document, gather, and aggregate data
- Overseeing the impact of AI on data security and privacy
- Guiding the development of operational and strategic plans to mitigate risks while exploring opportunities arising from AI technologies

Audit Committee evaluations should determine how AI could heighten risk if it fails, is intentionally or unintentionally misused, or is over relied upon, including potential impacts on financial reporting, compliance failures, and legal issues. This information helps Audit Committee members understand how their bank is using AI so they can guide discussions and challenge leadership when necessary. To drive this oversight, Audit Committee members should ask:

- How are we using AI to evaluate and take advantage of opportunities to grow and remain competitive in the markets we serve?
- What internal processes and controls are in place to regulate the use of AI, including formal procedures that ensure on-going human oversight?
- How are we driving the responsible use of AI through strong governance and risk management?
- Do our AI models use confidential or sensitive information and how is that data protected?
- Prior to their use are AI models tested and validated for security, accuracy, and data bias?
- How are employees trained on the appropriate use of AI?

AI technologies can be a powerful tool to transform your financial institution and deliver positive outcomes. Let our experts help your board and Audit Committee provide effective, comprehensive oversight. Contact Jessica Dore, CISA, at 989.797.8391 or Jessica.Dore@rehmann.com.

FFIEC Cybersecurity Assessment Tool Sunset

The Federal Financial Institutions Examination Council (FFIEC) sunset the Cybersecurity Assessment Tool (CAT) and removed it from the FFIEC website on August 31, 2025.

In 2015, Comptroller of the Currency Thomas J. Curry identified cyber threats as among the foremost risks facing banks. The FFIEC released the CAT self-assessment tool in 2015 as part of a three-prong approach to address this concern, along with information sharing and supervisory examinations. The CAT moved cybersecurity concerns outside a purely IT process by integrating them into governance and oversight functions with a framework that considered the cybersecurity lifecycle: identify what to protect, implement controls and processes to protect it, detect security breaches, respond to those breaches, and recover what was compromised.

Over the past decade, several new and updated government and industry resources have become available to guide cybersecurity risk assessments, support effective controls, evaluate vulnerabilities, and implement preparedness programs. The tools also keep management informed of continually evolving cyber security risks such as social engineering, ransomware, internal threats, third-party access to systems and networks, misuse of AI, and others.

These governmental resources include the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 and the 2023 Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Performance Goals. CISA is preparing to release Cybersecurity Performance Goals for the Financial Sector later this year. Industry-developed resources include the Cyber Risk Institute's (CRI) Cyber Profile and the Center for Internet Security Critical Security Controls.

To drive this oversight, Audit Committee members should ask:

1. What framework has the institution transitioned to?
2. Where is management at in the transition?
3. What was identified as part of the implementation of the new framework?
4. What are the third-party (vendor) impact/risks, and have they been addressed?

For guidance on implementing the best cyber risk assessment tools and controls for your financial institution, contact Jessica Dore, CISA, at 989.797.8391 or Jessica.Dore@rehmann.com.

Rehmann is a financial services and business advisory firm. We excel at helping clients because we take a collaborative, personalized approach and build a customized team of specialists to help them achieve their objectives. We focus on the business of business — allowing people to focus on what makes them extraordinary. The firm started as a CPA firm more than 75 years ago. Now, we are a multifaceted advisory firm that helps businesses and high-net-worth families maximize potential. Clients who work with us want us to be more than a vendor. They want collaboration, innovation, and continuous improvement.

Rehmann
EMPOWER YOUR PURPOSE®