Speakers for SMF Only

	Topic	Speaker	Firm	Fee/Regs
1.	1. Strategic Staffing Discussion Every organization is only as good as the people that work for it. This presentation will discuss current staffing challenges and offer solutions to address them. We will think strategically about how to address some of banks' biggest challenges. Topics discussed will include: i) succession of leadership and key positions; ii) improving/maintaining employee moral; iii) how to get the best out of every generation in the workplace; and iv) measuring success. 2. Regulatory Updates As always, banks are subject to numerous regulations that are always changing. This presentation will address current/recent changes, what challenges they present, and best practices for compliance. 3. Bank Examination/Enforcement Actions This presentation will discuss trends in bank examination and recent enforcement actions in the industry. 4. Update on Crypto and CBDC Since the Securities and Exchange Commission approved investment in cryptocurrencies from institutional investors the market cap of cryptocurrencies has skyrocketed. Additionally, central bank digital currency is dormant, but not gone. This presentation will update on current developments and how it affects banking.	Miles Pringle	The Bankers Bank	N/A
2.	Monetary Policy, Fiscal Policy, Economic Outlook 1- What is driving monetary policy decisions now? Inflation is continuing to moderate bringing the Fed's mandate on full employment into greater focus. 2- Is the deficit a problem? Depends on who you ask but the bond market will be the final arbiter. What signs do we need to be looking for as we think about the possible return of the "bond vigilantes"? Does anyone in Washington care? 3- The post-pandemic economy has been incredibly resilient. A snapshot of the economy today looks pretty good, but how much airbrushing is it taking to make the economy look good and is this airbrushing sustainable? 4- What are the implications of our bi-furcated banking system? The gulf between SIFI and non-SIFI banks seems wide.	Steve Wyett	BOKF	N/A
3.	1. Wire and Check Fraud (we are seeing a resurgence in both types including very creative criminals) • Key recent cases • Best practices to prevent 2. Regulatory Update: • Current Regulatory Actions and Trends (CFPB, FDIC, etc) • FinCen developments and financial crimes • Update on Fair Lending and Lending Discrimination Actions • Best Practices for servicing of SBA, FSA and USDA Guaranteed Loans 3. Current Issues in Account and Loan Operations: • Collateral Perfection Issues • Best Practices for Avoiding Lender Liability in Today's Environment	Joel Harmon, Zane Anderson, or one or more other Crowe & Dunlevy attorneys	Crowe & Dunlevy (sponsoring breakfast)	N/A

Speakers for SMF Only

	4. General Legal Update 5. Any other legal topic the OBA feels current or needed			
4.	Examiner Hot Spots and Regulatory Concerns for Community Banks	Lori Jackson	Forvis Mazars LLP	2 Nights Hotel
5.	1. Current Hiring and Compensation Trends in Oklahoma Specific to Banking *(all levels)* • Current hiring trends and compensation for all levels of professionals in Banking • Where we see the trends going in the next 3-5 years • How does OK stack compare to the rest of the south-central region • How is compensation reflected in hiring trends 2. People Strategy – How to Recruit and Retain Top Talent • Hiring strategy and compensation development (including incentives) • In office vs. hybrid vs. remote • Benefits and other perks • Work environment and culture • Upward mobility and growth opportunities • Visibility and forward vision 3. How to Select Your Board of Directors • Ideal expertise for the BOD • Ideal candidates for the BOD • Ideal size of your BOD • How best to define BOD compensation and responsibilities 4. Growing Organizations – When is it Time to Hire In-House Talent vs Consultants • Key differences between in-house and consultants • Key growth metrics to meet when considering in-house v. consultants • Cost benefit analysis on when to move from consultants to in-house • How to transition your organization from consultant reliant to self sufficient 5. Succession and Contingency Planning • Why it matters • Departure – Defined Succession Plan • Emergency/Interim Succession Plan • Stakeholder feedback • The board of directors' role • Streamlining personnel tasks • The solutions • Strategic Leadership Development • Tools for contingency planning and succession planning, (9-box, graph)	Emily De La O & Marco Gonzalez	Forvis Mazars LLP	_____

Speakers for SMF Only

6.	1. The Top 6 Controls to Reduce Your Risk of a Cyber Incident Cyber attacks are CEOs #1 fear in 2022, according to PWC's annual CEO survey. If you read the news headlines regularly, one can understand why. However, a huge gap exists between most organization's cybersecurity capabilities and the fear of a data breach or ransomware. So, what should your organization do to close the gap and reduce your cyber risk? This session will discuss the Top 6 Controls your organization should be implementing to significantly reduce your risk of a cyber attack. We'll walk through some of the most probably cyber attack scenarios and demonstrate how these top controls can mitigate your cyber risk, as well as discuss some additional risk-mitigating options every organization should consider 2. Creating a Culture of Cybersecurity at Your Institution The human element of information security is an increasing target for cybercriminals and generally considered the weakest area in information security. Security awareness and training on proper security protocols is an essential element of a strong cybersecurity program and regulatory compliance, but moving from reactive training to proactive training is the hard part. We will discuss many methods of constructing an adequate security awareness and training program for both employees of your organization and customers of your online products and services, including awareness to cybersecurity issues, training on what is expected, and clear accountability for employees and management responsible for protecting customer information. These elements can help establish a lasting culture that includes a passion for protecting customer information and a desire to be successful against cybercrime. In this session, we'll break down some of best practices to follow when providing training to employees and building a culture of cybersecurity, including: • People, Process, and Technology • Why People break rules • Training topics and tactics • Accountability for Security Awareness Training tests • Building a Culture of Cybersecurity 3. The Future of Cybersecurity: Trends You Should Know and Monitor The world of technology is very different today than it was just 5 years ago. From the technologies we use (cloud computing) to the threats we face (Ransomware, BEC) to the way we protect our data (MFA, Zero Trust), the cybersecurity landscape continues to evolve rapidly. It's highly likely that we'll look back 5 years from now and talk about how different our technologies and protections are today compared to back then. In this session, we'll discuss the continued evolution and trends in cybersecurity we believe are likely to occur in the next few years, including: • Cloud Computing Adoption • Continued reliance on Vendors (Vendor Management Machine Learning and Artificial Intelligence • Advanced Cybersecurity Controls (Zero Trust, Behavioral Analytics, Automation, Threat Hunting) • Future/Evolving Threats • Customer Adoption of Technologies 4. You Are A Technology Company As your organization is reviewing its strategic plans, take a moment to evaluate the use of technology as a core component of your business. If most of you are being honest with	Jon Waldman	SBS CyberSecurity	$2,500+travel

	yourselves, you will realize that your organization has shifted from performing a service for a customer and using technology to make that service more convenient to truly operating as a technology company that offers your customer a specific service. Look at it this way: if the majority of your customer interactions involve some component of technology, whether it's through online banking, mobile payments, other mobile applications, email, your internet-based telephones (VoIP), looking up customer information in your CRM or other software, you are a technology company. In this session, we will discuss the following: • Embracing Your Technology Company Status • Changing Your View of Cybersecurity • Acting Like a Technology Company			