Risk Factors Comparison 2023-11-29 to 2022-11-23 Form: 10-K

Legend: **New Text** ~~Removed Text~~ Unchanged Text Moved Text Section

Commercial and industrial loans are primarily made based on the identified cash flow of the borrower and secondarily on the collateral underlying the loans. The borrowers' cash flow may prove to be unpredictable, and collateral securing these loans may fluctuate in value. Most often, this collateral consists of accounts receivable, inventory and equipment. Significant adverse changes in a borrower' s industries and businesses could cause rapid declines in values of, and collectability associated with, those business assets, which could result in inadequate collateral coverage for our commercial and industrial loans and expose us to future losses. In the case of loans secured by accounts receivable, the availability of funds for the repayment of these loans may be substantially dependent on the ability of the borrower to collect amounts due from its clients. Inventory and equipment may depreciate over time, may be difficult to appraise, may be illiquid and may fluctuate in value based on the success of the business. If the cash flow from business operations is reduced, the borrower' s ability to repay the loan may be impaired. An increase in valuation allowances and charge- offs related to our commercial and industrial loan portfolio could have an adverse effect on our business, financial condition, results of operations and future prospects. Risks Related to Cybersecurity, Third Parties, and Technology **.** The occurrence of any information system failure or interruption, breach of security or **cyberattack** ~~cyber- attack~~ , at the Company, at its third- party service providers or counterparties may have an adverse effect on our business, reputation, financial condition and results of operations. Information systems are essential to the conduct of our business, as we use such systems to manage our customer relationships, our general ledger, our deposits and our loans. In the normal course of our business, we collect, process, retain and transmit (by email and other electronic means) sensitive and confidential information regarding our customers, employees and others. We also outsource certain aspects of our data processing, data processing operations, remote network monitoring, engineering and managed security services to third- party service providers. In addition to confidential information regarding our customers, employees and others, we, and in some cases a third party, compile, process, transmit and store proprietary, non- public information concerning our business, operations, plans and strategies. Information security risks for financial institutions continue to increase in part because of evolving technologies, the use of the ~~Internet~~ **internet** and telecommunications technologies (including mobile devices) to conduct financial and other business transactions and the increased sophistication and activities of organized crime, perpetrators of fraud, hackers, terrorists and others. Cyber criminals use a variety of tactics, such as ransomware, denial of service, and theft of sensitive business and customer information to extort payment or other concessions from victims. In some cases, these attacks have caused significant impacts on other businesses' access to data and ability to provide services. We are not able to anticipate or implement effective preventive measures against all incidents of these types, especially because the techniques used change frequently and because attacks can originate from a wide variety of sources, including attacks on third **-** party vendors and their applications and products used by the Bank. We use a variety of physical, procedural and technological safeguards to prevent or limit the impact of system failures, interruptions and security breaches and to protect confidential information from mishandling, misuse or loss, including detection and response mechanisms designed to contain and mitigate security incidents. However, there can be no assurance that such events will not occur or that they will be promptly detected and adequately addressed if they do, and early detection of security breaches may be thwarted by sophisticated attacks and malware designed to avoid detection. If there is a failure in or breach of our information systems, or those of a third- party service provider, the confidential and other information processed and stored in, and transmitted through, such information systems could be jeopardized, or could otherwise cause interruptions or malfunctions in our operations or the operations of our customers, employees, or others. Our business and operations depend on the secure processing, storage and transmission of confidential and other information in our information systems and those of our third- party service providers. Although we devote significant resources and management focus to ensuring the integrity of our information systems through information security measures, risk management practices, relationships with threat intelligence providers and business continuity planning, our facilities, computer systems, software and networks, and those of our third- party service providers, may be vulnerable to external or internal security breaches, acts of vandalism, unauthorized access, misuse, computer viruses or other malicious code and **cyberattacks** ~~cyber- attacks~~ that could have a security impact. In addition, breaches of security may occur through intentional or unintentional acts by those having authorized or unauthorized access to our confidential or other information or the confidential or other information of our customers, employees or others. While we regularly conduct security and risk assessments on our systems and those of our third- party service providers, there can be no assurance that their information security protocols are sufficient to withstand a **cyberattack** ~~cyber- attack~~ or other security breach. Across our industry, the cost of minimizing these risks and investigating incidents has continued to increase with the frequency and sophistication of these threats. ~~To date~~ **During June 2023** , **a third-party service provider (the" Service Provider") to the Bank advised the Bank that files with personally identifiable information related to Bank customers had been compromised during a security incident experienced by the Service Provider (the" Incident"). The Bank used the Service Provider to process transactions. The Incident resulted from a zero- day vulnerability in a managed file sharing software called MOVEit. MOVEit is used by thousands of organizations around the world for securely transferring sensitive and confidential information and** ~~the~~ **other** ~~Company~~ **data. The vulnerability was exploited in a large- scale, cyber campaign that impacted government agencies, universities, and corporations around the world. As a result of the Incident, an unauthorized party was able to obtain access to certain Bank customers' data in the Service Provider' s possession that contained social security numbers, account numbers, and other personally identifiable information. The Bank confirmed the Service Provider** has ~~no knowledge of a~~

~~material information~~ **fixed the vulnerability noted above and the Bank has implemented additional** security ~~breach affecting~~ **procedures when sharing files with the Service Provider. When the Bank received notice of the Incident from the Service Provider, the Bank promptly enacted response protocols. The Service Provider has provided appropriate notifications to potentially affected customers. The Bank worked with the Service Provider to identify any others potentially impacted by the Incident. The Bank** ~~its~~ **is** ~~systems~~ **not aware of any other third- party incidents related to the MOVEit vulnerability that has affected personally identifiable information associated with Bank customers** . The occurrence of any of the foregoing could subject us to litigation or regulatory scrutiny, cause us significant reputational damage or erode confidence in the security of our information systems, products and services, cause us to lose customers or have greater difficulty in attracting new customers, have an adverse effect on the value of our common stock or subject us to financial losses that may not be covered by insurance, any of which could have an adverse effect on our business, financial condition and results of operations. As information security risks and cyber threats continue to evolve, we may be required to expend significant additional resources to further enhance or modify our information security measures and / or to investigate and remediate any information security vulnerabilities or other exposures arising from operational and security risks. Furthermore, there continues to be heightened legislative and regulatory focus on privacy, data protection and information security. New or revised laws and regulations may significantly impact our current and planned privacy, data protection and information security- related practices, the collection, use, sharing, retention and safeguarding of consumer and employee information, and current or planned business activities. Compliance with current or future privacy, data protection and information security laws could result in higher compliance and technology costs and could restrict our ability to provide certain products and services, which could have an adverse effect on our business, financial condition and results of operations. Our customers are also targets of **cyberattacks** ~~cyber- attacks~~ and identity theft. There continues to be instances involving financial services and consumer- based companies reporting the unauthorized disclosure of client or customer information or the destruction or theft of corporate data. Large scale identity theft could result in customers' accounts being compromised and fraudulent activities being performed in their ~~name~~ **names** . We have implemented certain safeguards against these types of activities **,** but they may not fully protect us from ~~fraudulent~~ financial losses. The occurrence of a **security** breach ~~of security~~ involving our customers' information, regardless of its origin, could damage our reputation and result in a loss of customers and business ~~and~~ **,** subject us to additional regulatory scrutiny, and ~~could~~ expose us to litigation and possible financial liability. Any of these events could have an adverse effect on our **business,** financial condition and results of operations. Third **-** party vendors subject the Company to potential business, reputation and financial risks. Third **-** party vendors are sources of operational and information security risk to the Company, including risks associated with operations errors, information system interruptions or breaches, and unauthorized disclosures of sensitive or confidential customer information. The Company requires third **-** party vendors to maintain certain levels of information security; however, vendors may remain vulnerable to breaches, unauthorized access, misuse, computer viruses, and / or other malicious attacks that could ultimately compromise sensitive information. We have developed procedures and processes for selecting and monitoring third **-** party vendors, but ultimately are dependent on these third **-** party vendors to secure their information. If these vendors encounter any of these types of issues, or if we have difficulty communicating with them, we could be exposed to disruption of operations, loss of service or connectivity to customers, reputational damage, and litigation risk that could have an adverse effect on our business, financial condition and results of operations. The failure of an external vendor to perform in accordance with the contracted arrangements under service level agreements, because of changes in the vendor' s organizational structure, financial condition, support for existing products and services or strategic focus or for any other reason, could be disruptive to our operations, which could have an adverse effect on our business and, in turn, our financial condition and results of operations. Additionally, replacing certain third **-** party vendors could also entail significant delay and expense. We are heavily reliant on technology, and a failure to effectively implement technology initiatives or anticipate future technology needs or demands could adversely affect our business or performance. Like most financial institutions, the Bank significantly depends on technology to deliver its products and ~~other~~ services and to otherwise conduct business. To remain technologically competitive and operationally efficient, the Bank invests in system upgrades, new technological solutions, and other technology initiatives. Many of these solutions and initiatives have a significant duration, are tied to critical information systems, and require substantial resources. Although the Bank takes steps to mitigate the risks and uncertainties associated with these solutions and initiatives, there is no guarantee that they will be implemented on time, within budget, or without negative operational or customer impact. The Bank also may not succeed in anticipating its future technology needs, the technology demands of its customers, or the competitive landscape for technology. If the Bank were to falter in any of these areas, it could have an adverse effect on our business, financial condition and results of operations. **In August 2023,** ~~There are operational and reputation risks associated with~~ the **Company** ~~planned digital transformation. Management is in the process of implementing~~ **implemented** a new core processing system (" digital transformation") ~~for the Bank, which is expected to be operational by September 2023~~ . ~~The~~ **While the** digital transformation **was completed successfully,** ~~is expected to better position~~ the **Company** ~~Bank for the future and allow for the introduction of new products and services to enhance customer experiences. This project~~ may **face** ~~subject the Company to~~ operational risks, such as disruptions in technology systems **, which may** ~~impacting~~ -- **impact** customers. The Company will work to remediate any such disruptions, if they occur, but no assurance can be given that a potential adverse development will be quickly or completely remediated. If an adverse development arising from the digital transformation is not sufficiently remediated or is not remediated in a timely fashion, the Company' s reputation could be significantly impacted **,** which could result in loss of customer business, subject the Company to regulatory scrutiny, or expose the Company to ~~possible~~ litigation, any of which could have a material impact on the Company' s financial condition and results of operations. Risks Related to Competition Strong competition may limit growth and profitability. While we are one of the largest mortgage loan originators in the state of Kansas, we compete in the same market areas as local, regional, and national banks, credit unions, mortgage brokerage firms, investment banking firms, investment brokerage firms **, mortgage bankers** ,

and savings institutions. We also compete with online investment and mortgage brokerages and online banks that are not confined to any specific market area. Many of these competitors operate on a national or regional level, are a conglomerate of various financial services providers housed under one corporation, or otherwise have substantially greater financial or technological resources than the Bank. We compete primarily on the basis of the interest rates offered to depositors, the terms of loans offered to borrowers, and the benefits afforded to customers as a local institution and portfolio lender. Should we face competitive pressure to increase deposit rates or decrease loan rates, our net interest income could be adversely affected. Additionally, our competitors may offer products and services that we do not or cannot provide, as certain deposit and loan products fall outside of our accepted level of risk. Our profitability depends upon our ability to compete in our local market areas. Risks Related to Regulation We operate in a highly regulated environment which limits the manner and scope of our business activities, and we may be adversely affected by new and / or changes in laws and regulations or interpretation of existing laws and regulations. We are subject to extensive regulation, supervision, and examination by the OCC, the FRB, and the FDIC. These regulatory authorities exercise broad discretion in connection with their supervisory and enforcement activities, including the ability to impose restrictions on a bank' s operations, reclassify assets, determine the adequacy of a bank' s ACL, and determine the level of deposit insurance premiums assessed. The CFPB has broad powers to supervise and enforce consumer protection laws, including a wide range of consumer protection laws that apply to all banks and savings institutions, like the authority to prohibit " unfair, deceptive or abusive " acts and practices. The CFPB also has examination and enforcement authority over all banks with regulatory assets exceeding $ 10 billion at four consecutive quarter- ends. The Bank ~~has~~ **exceeded $ 10 billion in regulatory assets at March 31, 2023, June 30, 2023 and September 30, 2023. The Bank intends to be below $ 10 billion in regulatory assets at December 31, 2023 so it will** not ~~exceeded~~ -- **exceed** $ 10 billion in regulatory assets at four consecutive quarter- ends **. There are increased direct costs** , ~~but~~ **additional regulatory burdens with indirect costs, and lost revenue, mainly related to interchange fees, associated with the Bank being over $ 10 billion in regulatory assets at certain points in time and for four consecutive quarter- ends. As long as the Bank does not exceed $ 10 billion in regulatory assets for four consecutive quarter ends,** it ~~may at some point in the future. Smaller banks, like the Bank,~~ will continue to be examined for compliance with ~~the~~ consumer **protection** laws and **the** regulations of the CFPB by ~~their~~ -- **the Bank' s** primary bank ~~regulators~~ - **regulator** ~~(~~ **,** the OCC ~~, in the case of the Bank)~~ . The Dodd- Frank Act also weakens the federal preemption rules that have been applicable for national banks and federal savings associations and gives state attorneys general the ability to enforce federal consumer protection laws. Any change in such regulation and oversight, whether in the form of regulatory policy, regulations, legislation, interpretation or application, could have an adverse impact on our operations. Moreover, bank regulatory agencies have been active in responding to concerns and trends identified in examinations and have issued formal enforcement orders requiring capital ratios in excess of regulatory requirements and / or assessing monetary penalties. Bank regulatory agencies, such as the OCC, the FRB and the FDIC, govern the activities in which we may engage, primarily for the protection of depositors **' funds, the DIF and the safety and soundness of the banking system as a whole** , and not for the protection or benefit of investors. The CFPB enforces consumer protection laws and regulations for the benefit of the consumer and not the protection or benefit of investors. In addition, new laws and regulations, including those related to environmental, social, and governance initiatives, may continue to increase our costs of regulatory compliance and of doing business, and otherwise affect our operations. New laws and regulations may significantly affect the markets in which we do business, the markets for and value of our loans and securities, the products we offer, the fees we can charge and our ongoing operations, costs, and profitability. The Company is also directly subject to the requirements of entities that set and interpret accounting standards such as the Financial Accounting Standards Board, and indirectly subject to the actions and interpretations of the Public Company Accounting Oversight Board, which establishes auditing and related professional practice standards for registered public accounting firms and inspects registered firms to assess their compliance with certain laws, rules, and professional standards in public company audits. These regulations, along with ~~the currently~~ existing tax, accounting, securities, and monetary laws, regulations, rules, standards, policies and interpretations, control the methods by which financial institutions and their holding companies conduct business, engage in strategic and tax planning, implement strategic initiatives, and govern financial reporting. The Company' s failure to comply with laws, regulations or policies could result in civil or criminal sanctions and money penalties by state and federal agencies, and / or ~~reputation~~ **reputational** damage, which could have an adverse effect on the Company' s business, financial condition and results of operations. See" Part I, Item 1. Business- Regulation and Supervision" for more information about the regulations to which the Company is subject. Other Risks The Company' s ability to pay dividends is subject to the ability of the Bank to make capital distributions to the Company. The long- term ability of the Company to pay dividends to its stockholders is based primarily upon the ability of the Bank to **generate earnings and to, therefore,** make capital distributions to the Company, and on the availability of cash at the holding company level in the event earnings are not sufficient to pay dividends. Under certain circumstances, capital distributions from the Bank to the Company may be subject to regulatory approvals. See" Item 1. Business – Regulation and Supervision" for additional information. Our risk management and compliance programs and functions may not be effective in mitigating risk and loss. We maintain an enterprise risk management program that is designed to identify, quantify, monitor, report, and control the risks that we face. These risks include: interest- rate, credit, liquidity, operations, reputation, compliance and litigation. We also maintain a compliance program to identify, measure, assess, and report on our adherence to applicable laws, policies and procedures. While we assess and improve these programs on an ongoing basis, there can be no assurance that our risk management or compliance programs, along with other related controls, will effectively mitigate all risk and limit losses in our business. If conditions or circumstances arise that expose flaws or gaps in our risk management or compliance programs, or if our controls do not function as designed, the performance and value of our business could be adversely affected. **The Company may not be able to attract and retain skilled employees. The Company' s success depends, in large part, on its ability to attract and retain key people. Competition for the best people can be intense, and the Company spends considerable time and**

resources attracting and hiring qualified people for its operations. The unexpected loss of the services of one or more of the Company' s key personnel could have an adverse impact on the Company' s business because of their skills, knowledge of the Company' s market, and years of industry experience, as well as the difficulty of promptly finding qualified replacement personnel.