Disclosures Regarding Electronic Communications and Monitoring

1. Electronic Communications

University Bank ("University Bank," "we," "us," or "our") is a Michigan state-chartered financial institution and a member of the Federal Deposit Insurance Corporation (FDIC). When you visit our website or the websites of any of our divisions or subsidiaries, or use our electronic services, you may transmit electronic communications to us, including, but not limited to, emails, secure messages, form submissions, transaction-related communications, and related information (collectively, "electronic communications").

To protect our customers, employees, systems, and information, and to comply with applicable federal and state law, **University Bank may monitor, intercept, record, store, access, and review electronic communications**, as permitted by law. Monitoring is conducted for purposes that include information security, fraud prevention, risk management, quality assurance, regulatory compliance, recordkeeping, and customer service.

2. Storage and Retention of Communications

Electronic communications and related information may be **stored and retained** in accordance with University Bank's record retention policies and applicable legal and regulatory requirements, including those applicable to insured financial institutions. Retention periods vary depending on the type of communication and governing law.

3. Disclosure of Electronic Communications

University Bank may disclose electronic communications and related information:

- To third-party service providers that perform services on our behalf and are subject to confidentiality and information security obligations;
- As required or permitted by applicable federal or Michigan law, regulation, or legal process;
- To regulators, law enforcement agencies, or governmental authorities with appropriate legal authority; or
- To protect the rights, property, safety, or security of University Bank, our customers, or others.

4. Terms Applicable to Website Use

Consent to Electronic Monitoring and Interception

By accessing or using this website or the websites of any of our divisions or subsidiaries, or any electronic service provided by University Bank or any of its divisions or subsidiaries, **you knowingly and voluntarily consent to the monitoring, interception, recording, access, and use of electronic communications and related information** transmitted to or from University Bank systems to the extent permitted by applicable law.

This consent applies to communications transmitted through any device used to access services provided by University Bank or any of its divisions or subsidiaries, including computers, mobile devices, and other electronic equipment.

No Expectation of Absolute Privacy

Although University Bank employs administrative, technical, and physical safeguards designed to protect information, **no electronic communication transmitted over the Internet or stored on electronic systems can be guaranteed to be completely private or secure**.

5. Terms Applicable to Messaging

Secure Messaging Notice

Messages sent through University Bank's online banking platform or secure message center are intended for customer service and account-related communications. Such messages **may be monitored, accessed, stored, and reviewed** by authorized University Bank personnel for security, operational, compliance, recordkeeping, and service-related purposes. Please do not submit highly sensitive personal information through secure messaging unless specifically requested by University Bank.

6. System Security, Fraud, and Network Monitoring

System and Security Monitoring

To protect customers and comply with applicable banking, cybersecurity, and safety and soundness requirements, University Bank maintains safeguards designed to secure its information systems and prevent unauthorized activity. As part of these efforts, University Bank may collect and analyze technical and usage information, including IP addresses, device identifiers, access times, and session activity, to detect fraud, manage risk, and maintain system integrity.