Privacy of Consumer Information, Information Security and Cyber Security

Banner Bank and its subsidiaries ("Banner") take its fiduciary responsibilities seriously to preserve, improve and account for company information and information systems, which are recognized as critical company assets. The Bank has programs in place to ensure that information and information systems are properly protected from a variety of threats, including error, fraud, embezzlement, improper disclosure, sabotage, terrorism, extortion, industrial espionage, privacy violation, service interruption and natural disaster.

Banner's policies and procedures are intended to:

* ENSURE THE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF BANNER DATA – BY means of comprehensive security policies, processes, and technologies that allow for the proper protection of data and that facilitate secure, robust access.

* CONTINUALLY MAINTAIN A SCALABLE, SECURE AND RELIABLE PRODUCTION ENVIRONMENT – By means of advanced security processes and technologies to facilitate comprehensive attack identification, analysis, and response in a coordinated and efficient manner across the bank.

* ESTABLISH SECURITY TO PROTECT AND ENABLE THE BANK - BY embracing more effective and secure technologies and processes that result in reduction or elimination of inefficiencies within the IT environment and across the bank.

* ESTABLISH A MUTUAL CULTURE OF SECURITY – By creating a secure environment and a strong alliance with all employees in the practice of information security.

PRIVACY OF CONSUMER INFORMATION

Banner Bank and its subsidiaries ("Banner") is committed to safeguarding and sharing of non-public consumer information as required with the various laws and regulations that affect consumer information including the Gramm-Leach-Bliley Act (GLBA).

It is the policy of Banner Bank that both the financial records of our customers and the relationships between the Bank and our customers are confidential, and that customer non-public personal information shall not be disclosed to third parties, without first providing a privacy notice compliant with regulatory requirements. The Privacy Policy is reviewed and approved annually by members of the Board of Directors. Customers initially receive our Privacy Notice when opening a new deposit account or loan, credit card or safe deposit box. The Notice describes Banner's information sharing practices and when the client can limit that sharing.

Access to customer information are restricted to those employees who require the same in order to provide products or services. Certain state privacy regulations allow for the customer to request what personal information is being collected, the right to opt out of allowing the bank to sell the personal

information to third parties, the right to request deletion of any personal information and the right to equal service and pricing.

Banner employees receive annual training on Banner's privacy policy, including opt out and do not call procedures.

INFORMATION SECURITY (Confirm statements with Karl P)

Management shall, from time to time, identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of organization owned or managed information or information systems. Areas of physical, administrative, and technical risks will be assessed for potential impact and likelihood. Security controls in place to mitigate the resultant risks of identified threats will be evaluated and risks will be deemed either acceptable, according to the risk profile of the organization, or unacceptable. Unacceptable risks are to be addressed by identifying and implementing appropriate corrective actions.

Information security training is conducted annually. Specific topics such as phishing, vishing and other social engineering testing are addressed. Managers are held accountable for ensuring that employees complete all required courses.

To make sure that our employees remain vigilant, and that data security is always top of mind, we regularly stage "phishing" tests, sending seemingly innocuous emails that may contain viruses or dangerous links to our employees to be sure that they handle cyberthreats appropriately. In the event an employee fails a test, we provide re-training and work with the employee and their manager to increase awareness.

CYBER SECURITY

Our systems environment adheres to all applicable laws regarding digital security. Vulnerability testing is conducted quarterly. Banner Corporation may engage outside security expertise, as appropriate, to assist in such vulnerability testing.

All third party vendors providing information systems application services are monitored using a prescribed vendor management process. The process will include review of the vendor's financial condition, strategy to offer continued services, information security audits and controls, business continuity planning and disaster recovery testing initiatives, and current contract compliance. Any vendor using sub service-contractors (Fourth Party Contractors) shall require sub service-contractors to adhere to all terms and conditions of the contract in place between vendor and Banner Bank. Sub service-contractors are monitored following the Bank vendor management process.