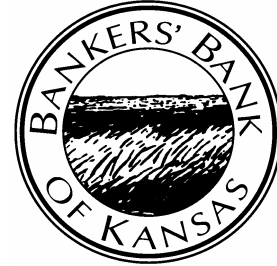


Bankers' Bank of Kansas
2007 Compliance Statement





2007 Compliance Statement

Table of Contents

- 1- Statement of Preparedness
- 2- ABIL Web Security
- 3- BBOK Data Security Statement of Policy
- 4- Policy Incident Response
- 5- Response Program for Unauthorized Access to Customer Information and Customer Notice
- 6- Safeguards for Protecting Customer Information
- 7- OFAC Compliance Statement

Statement of Preparedness

Bankers' Bank of Kansas is proactive in its efforts to manage the risks related to the protection of customer information, the ability to manage an interruption in business, and has a system in place to adequately assess the risks of third party vendors with whom we do business.

- **BBOK engages an independent auditor to review its financial statements and operating procedures.**
- **BBOK maintains an internal audit program that reports regularly to the Board of Directors.**
- **BBOK engages a third party for independent penetration of its data systems and information security risk assessment.**
- **BBOK has Board approved Information Security Policies and Privacy Policies.**
- **BBOK has a Board approved Risk Management Program.**
- **BBOK has a Board approved disaster recovery program that has been tested.**
- **BBOK is a National Bank and a member of the Federal Reserve System. BBOK is required to comply with all appropriate regulations and standards.**

We welcome any customer to visit our office in relation to any risk management related issues.

ABIL Web Security

Bankers' Bank of Kansas, N.A. has taken strong steps to provide our customers an Internet-based communications system that provides the strictest protection against damage to their systems, while housing the Host in a physically secure location in our institution.

Host Security

At BBOK, the ABIL Web Host is securely located behind a combination-locked door. The Internet connection is available only during business hours.

The ABIL Web Host resides on our Network, securely placed behind our Firewall and IDS. Passwords are required at the Host (for the network, and for the application) prior to initializing ABIL Web in the morning, and once again prior to posting any data for customer retrieval. After 15 minutes of inactivity, ABIL Web will automatically log the user off of the system.

Customer Security

Users are issued a Sign-on ID and required to designate a password that expires every 30 days. Users are given rights to specific applications, as well as dollar limits for each transaction type. Customers are allowed access to ABIL Web after verification of ID, Password, and Digital Certificate authenticity.

Encryption

Customers connecting to the Host via an Internet connection are only allowed access after verification of a Sign-on ID, password and previously issued digital certificate. The data being passed is encrypted using SSL software, and then transmitted through the Internet using 128-bit encryption.

BBOK Data Security Statement of Policy

Objective

The purpose of this policy is to establish mechanisms to provide reasonable assurance of the protection of data in all its forms and media through an appropriate classification according to its level of criticality. In addition, it also establishes guidelines for the proper handling of sensitive data.

Data Ownership

Data Owners will be identified for all major information assets and the responsibility and accountability for the maintenance of appropriate controls will be assigned. Data Owners identify and maintain information and information systems within their assigned area of control. Each Data Owner must understand the uses and risks associated with the information for which they are accountable.

Data Classification

In order to ensure the security of information in all its forms and media, BBOK categorizes the sensitivity of information into categories of “public, internal use only and confidential” in order that the information will be protected from unauthorized disclosure, use, modification and deletion.

Data Handling

All users will observe the specific requirements outlined for the proper handling of sensitive information. If confidential information is lost, is disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, the Data Owner and the Vice-President, Technology Officer will both be notified immediately and appropriate action taken based on the compromise situation.

Data Security Monitoring

The Network firewall, intrusion detection system and anti-virus will be continually and consistently monitored by an outside vendor on a 24/7/365 basis. The logs generated from the firewall are secured and available for review upon management request by qualified and authorized personnel. A Network Security Report is provided to the Board of Directors on a monthly basis.

The receipt of a signed non-disclosure agreement will always precede the disclosure of confidential information to consultants, contractors, and temporaries or other third parties.

Policy Incident Response

Objective

The purpose of this policy is to ensure that, in the event a security breach or other security-related event occurs, the appropriate action is taken to minimize and/or contain any potential damage that can occur as a result of the incident. It also serves to protect the organization's interests will legal action be taken against or by the organization.

Policy

It is the responsibility of the Vice-President, Technology Officer to establish incident response procedures that ensure a quick, effective and orderly response to security incidents and that provide guidance to the Computer Incident Response Team (CIRT). The CIRT team will be comprised of members from upper level management and the Vice-President, Technology Officer. The CIRT team is responsible for executing the incident response procedures outlined in this document.

Incident response procedures will provide guidance for handling all potential types of security incidents, including but not limited to:

- Unauthorized use (sending SPAM, chain e-mails or threatening e-mails, planting viruses, conducting network-level probes/scans, exceeding your authorization level, etc.).
- Theft of data.
- Alteration or deletion of data.
- Denial of service and/or system failure.
- Unsuccessful access attempts repeated in excess of defined thresholds.
- Unauthorized access that is manifested:
 - Internally (by an employee, customer or vendor on company property).
 - Externally (by an employee, customer, vendor and all others outside company property).

In addition the procedures will establish:

- Normal contingency plans (designed to recover systems or services as quickly as possible).
- Processes for analyzing and identifying the cause of the incident.
- Planning and implementation of remedies to prevent recurrence.
- Collection of audit trails and/or evidence.
- Communication with business users and others affected by or involved with the recovery from the incident.

Action to correct and recover from security breaches and system failures will be carefully and formally controlled. Procedures will ensure that:

- Only clearly identified and authorized staff are allowed access to live systems and data.
- All emergency actions are documented in detail.

- Emergency action is reported to management and reviewed in a timely and orderly manner.
- The integrity of business systems and security controls is confirmed with minimal delay.

To provide evidence for investigation, prosecution, and disciplinary actions, certain information will be captured whenever it is suspected that computer or network related crime or abuse has taken place. The relevant information will be securely stored off-line until such time as it is determined that the organization will not pursue legal action or otherwise use the information. The information to be immediately collected includes the system logs, application audit trails, other indications of the current system states, as well as copies of all potentially involved files.

To allow proper remedial action to be taken in a timely manner, records reflecting security relevant events will be periodically reviewed in a timely manner by the Vice-President, Technology Officer.

Response Program for Unauthorized Access to Customer Information and Customer Notice

Security Guidelines

The security guidelines for BBOK are designed to:

1. Ensure the security and confidentiality of customer information.
2. Protect against any anticipated threats or hazards to the security or integrity of such information.
3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

Risk Assessment and Controls

Our risk assessment takes into account the following:

1. Reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.
2. The likelihood and potential damage of threats, taking into consideration the sensitivity of customer information.
3. The sufficiency of policies, procedures, customer information systems and other arrangements in place to control risks.

BBOK's Information Security Program addresses the controls in place to safeguard customer information, to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.

BBOK has in place response programs that specify the actions to be taken when BBOK suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies.

Service Providers

The contracts will require the service providers to implement appropriate measures designed to protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer and to notify BBOK in a timely manner if such an incident occurs. If an incident of unauthorized access to customer information does occur, BBOK will make the determination, in conjunction with the service provider, as to which party will notify BBOK's customers and/or regulator. BBOK acknowledges that it is ultimately the responsibility of BBOK to notify its customers and regulator.

Components of a Response Program

If BBOK suspects or detects that unauthorized individuals have gained access to customer information in customer information systems maintained by BBOK or a service provider of BBOK, a response program has been implemented and will be applied as deemed appropriate for the situation and in accordance with the federal regulation.

- I. BBOK's response will be based on an investigation and evaluation of the following information:
 - What information has been compromised? Does it fall into the definition of "sensitive customer information"? Sensitive customer information means a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password or password and account number.
- II. As soon as practical following this discovery process, BBOK staff will notify the OCC, by phone, of the details of the incident.
- III. If appropriate, a SAR will be filed and law enforcement authorities will be notified.
- IV. Appropriate steps will be taken to contain and to control the incident. Once the scope of the incident has been established a plan will be determined for how to deal with the exposed accounts. As the situation warrants, a customer's credit card account, loan or other banking account may be closed, a new account issued, or the account may continue to be monitored until fraudulent activity occurs or the risk of fraud due to the incident has significantly decreased.
- V. If the results of the investigation warrant a notification, BBOK will determine if all customers will be notified or just those specifically impacted by the unauthorized access. The customer(s) will receive either a telephone call, electronic notification by email when authorized, or a written notice as soon as possible. The exception to "as soon as possible" notification would be if the notification would interfere with a criminal investigation and the law enforcement agency provides the institution with a written request for the delay. If written notice to the customer(s) is deemed necessary, the content of the notice will be accordance with federal regulations.

BBOK will train all staff that may be involved in a response to customer inquiries and requests for assistance.

Safeguards For Protecting Customer Information

The Board has approved the written information security program.

Safeguarding Sensitive Customer Information

The Credit Card department has dual control procedures in place for checking all new accounts, monetary and non-monetary transactions. Passwords and parameters restrict access by credit card employee to the FIS system. The cardholder files are kept in a secured room accessed by a security code. Only those employees with a "need to know" have the code and access to BBOK's internal system for scanned files.

The Loan department has dual control procedures in place for checking the input of new loans, changes and payments and the impact on GL accounts. All loan files are scanned. The loan files physically reside in a separate, locked room. Access to the ASI loan system is restricted by password to those employees with a "need to know".

The Electronic department has dual control procedures on all wire transfers. ACH and Savings Bonds for specific customers are handled via direct file interface between our intranet and the Federal Reserve Bank (FRB). Both intranet and FRB systems are accessible from designated workstations using various methods of multi layer authentication.

Employees in each area of the bank are trained to require specific information from the caller before providing any account information. If there is reason to suspect any given call, the call should be directed to a Supervisor or Manager. If the Supervisor or Manager believes the call is suspect, the President of Bankers' Bank will be informed and a decision made on how to proceed.

If any area of the bank is notified of an error or a complaint, the Error Resolution form and/or Inquiry/Complaint form, as appropriate, are available to use for documentation and tracking.

Disposal of Sensitive Customer Information

Each employee is responsible to safeguard information with which they work and/or to which they have access. Specifically, files with personal, nonpublic information such as cardholder files, loan files or operations information will be put away or locked each day. Care will be taken not to leave this type of information on computer screens when not in use.

Historical information, paper files or documentation that contains specific sensitive account information is shredded or deleted in accordance with KBA guidelines. BBOK utilizes shred bins located throughout the building. This information/documentation is shredded on site on a weekly basis by the security company.

OFAC COMPLIANCE STATEMENT

To assist you in maintaining and upholding the security of your bank's financial transactions via ABIL Web, Bankers' Bank of Kansas strongly encourages the checking of all such transactions against the OFAC Lists of Specially Designated Nationals and Blocked Persons (SDN List) and the non-SDN List titled NS-PLC.

While BBOK provides the tool, through ABIL Web, to check all incoming and outbound wires against the SDN and non-SDN List this does not take the place of an institution following its own internal procedures in the event of a match.

When BBOK receives outgoing transfers via ABIL Web, such checks are conducted as a matter of course before entrance into the Fed system or for any other type of processing. Likewise, any incoming transfers received from the Federal Reserve Bank are checked prior to being made available for download on ABIL Web. Domestic wires are scanned for the Originator and Beneficiary names. International wires are additionally scanned for country.

Your institution may further ensure security by utilizing the integrated OFAC scanner for wire transfers, regularly updated and available in your ABIL Web software. Upon receipt of, or prior to submission of, wire transfers via ABIL Web, the system will automatically check such transfers against the Lists. This check is an actual one-to-one match check. In doing so, you are provided an additional set of security measures supplementary to those already practiced by BBOK.

Should you discover a match between a transfer and the Lists, follow your bank's OFAC procedures for verification of a match. If appropriate, contact the Office of Foreign Assets Control at (202) 622-2480 or 800-540-6322. In the event that BBOK discovers a suspected or actual match with an incoming transfer, we will implement our OFAC procedures for Incoming Wire Transfers – including the notification of OFAC at the aforementioned number and the blocking or freezing of assets. Should a match be found in an outbound transfer from your bank, BBOK will implement our OFAC procedures for Outgoing Wire Transfers. We will contact your bank to inform you of the situation, confirm that the item is a match or false positive and, if appropriate, contact OFAC.

BBOK does not presume to give compliance or legal consultation regarding your bank's internal policy and procedures as it pertains to OFAC compliance.