Office of Controller of The Currency

OCC 2013-29
Subject: Third-Party Relationships
Date: October 30, 2013
Description: Risk Management Guidance

Summary
This bulletin provides guidance to national banks and federal savings associations (collectively, banks) for assessing and managing risks associated with third-party relationships. A third-party relationship is any business arrangement between a bank and another entity, by contract or otherwise.

Due Diligence and Third-Party Selection
A bank should conduct due diligence on all potential third parties before selecting and entering into contracts or relationships. A bank should not rely solely on experience with or prior knowledge of the third party as a proxy for an objective, in-depth assessment of the third party's ability to perform the activity in compliance with all applicable laws and regulations and in a safe and sound manner.

BTTF Response: **Vendor Due Diligence**: NAID AAA secure data destruction certificate: NAID certification is a recognized industry standard for the secure handling and destruction of sensitive information. This certification is an important "due diligence" document. The certification must be renewed annually and requires successfully passing an independent third party audit.

Legal and Regulatory Compliance
Evaluate the third party's legal and regulatory compliance program to determine whether the third party has the necessary licenses to operate and the expertise, processes, and controls to enable the bank to remain compliant with domestic and international laws and regulations. Check compliance status with regulators and self-regulatory organizations as appropriate.

BTTF Response: Legal and Regulatory Compliance: We are a State and Federal EPA permitted universal waste consumer electronics processing destination facility. NJ, NY, and CT law requires the recycling of all to be disposed of electronics by an authorized recycler. NJ and CT environmental regulations require a state issued permit to process/recycle electronics. Hard drive shredding, crushing or any other form of processing requires the DEP issued permit. Certification of NIST Guidelines for Media Sanitization compliance: Federal data privacy laws such as GLB require the destruction of sensitive data prior to the disposal of the data media. Destruction must meet NIST "Guidelines for Media Sanitization"

Business Experience and Reputation
Evaluate the third party's depth of resources and previous experience providing the specific activity. Assess the third party's reputation, including history of customer complaints or litigation. Determine how long the third party has been in business, its market share for the activities, and whether there have been significant changes in the activities offered or in its business model. Conduct reference checks with external organizations and agencies such as the industry associations,

BTTF Response: **Business Experience and Reputation:** BTTF has focused its secure data destruction services on the financial industry. Our banking customer reference list is extensive and includes the Federal Reserve System.

Insurance Coverage
Verify that the third party has fidelity bond coverage to insure against losses attributable to dishonest acts, liability coverage for losses attributable to negligent acts, and hazard insurance covering fire, loss of data, and protection of documents

Insurance Coverage: Certificate of Insurances. In addition to standard insurances we maintain $5M Insurance coverage for: Employee Dishonesty, Professional Liability and Pollution insurances.