TransportationInsight®
Evaluate. Innovate. Dominate.

Examine Potential High Risk Areas within the Auditing Process

"Overall, we found the set-up process quick and painless, and their method for identifying invoice errors and recovering refunds has saved us a significant amount of money that we would have never been able to recover on our own."

– Director of Operations, Industry Leader in Lamination

According to First Research, revenue for US transportation services is forecast to grow at an annual compounded rate of 5 percent between 2016 and 2020. Such large numbers equate to a substantial amount of data flowing through the carrier network. This data contains sensitive information such as financial records and customer addresses. To avoid the risk of a security breach, the data should be safeguarded. It should also be leveraged to make informed business decisions. Data can tell us the story of the current state and uncover potential opportunities for the future.

If you are utilizing a third party to audit your parcel shipments, you should make sure that your partner follows industry best practices to protect your company's money and information. These four areas that your partner should take very seriously are financial controls, personnel security, IT security and physical security.

Financial Controls

Shippers seeking to use a third party to manage their audit and pay process are faced with a decision about the financial controls within their partners' operations. Audit service providers should be vetted to see if they are protecting your money appropriately by confirming they offer:

- SSAE16 Type II Certification – a rigorous 3rd party audited certification
- Highly scrutinized, redundant, fund maintenance and management
- Multi-level fund oversight; Accounting Clerk to Controller
- Annual, independently audited financials
- Segregation of financial processes

The audit and pay process requires trust between shipper and provider - trust that involves a significant amount of funds advanced for payment to carriers on behalf of the shipper. Transportation Insight enhances trust with monthly reviews of clients' accounts. Escrow report and review occurs at the customer level to ensure complete transparency.

Personnel Security

To protect your company against a security breach, personnel security should be as rigorous as fiscal security. The people who handle your money and data should be beyond reproach to eliminate risk. Without this kind of security, audit companies can face fraud and embezzlement issues caused by employees who were not given:

- Background Checks
- Credit History Analysis
- Criminal Record Analysis
- Prior Education Analysis
- Confidentiality and Non-Disclosure Agreements

IT Security

Shippers everywhere should ensure that whomever they trust to manage their accounting and auditing service has the internal controls to prevent an information technology security breach. To protect your company, money and data, your audit provider and any related technologies should have:

- Published IT policies covering all aspects of the SSAE16 controls
- Restricted employee network access
- Recorded network login and activity logs
- Firewall protected Gateways
- Private and restricted VPN access
- Network intrusion detection
- Mandatory login – user name and password
- Multi-failure account Auto-lock
- Role and need access segmentation
- Minimum 256-bit security encryption protocol
- Regularly updated Anti-virus software
- Dangerous Email Scanning
- Complex and expiring password rules
- Employee data and financial security training
- Employee Turn-over shut offs
- Security patches current on all servers
- A current disaster recovery plan

Physical Security

Audit firms have your company's information in electronic format that may be accessed from computers on site as well as in data centers. They may also have some information in paper stored on premise in file cabinets or other locations. Physical security also should be a consideration to protect both physical assets as well as to protect electronic access to data. From cameras and monitoring equipment to alarm systems and key-coded entries - having physical security in place can prevent a number of threats. As with virtual access, placing the following limits on who has access to your physical location is crucial:

- Controlled access to facility entrances and exits
- Controlled access to office entrances and exits
- Video surveillance
- Alarm system
- Logging of access with routine reviews
- Authorized access list
- Identify verification
- Access badges
- Access segregation – access only to areas required
- Visitor/Temporary access controls
- Locks on file cabinets with restricted access

Audit companies handle large sums of money and sensitive information for their clients in the same way that medical and financial firms do. You should be sure your partners have all four security areas covered: Financial Controls, Personnel Security, IT Security and Physical Security. They should hold themselves to the same stringent standards of security and protection standards of security as financial and health institutions; just like Transportation Insight does. We have the added protection and experienced staff to audit and pay customers' invoices efficiently, accurately and most importantly securely.

Operating Centers and Client Support Locations across North America

Corporate Hickory, NC
Atlanta, GA
Bentonville, AR
Boston, MA
Charlotte, NC
Omaha, NE
Salt Lake City, UT

TransportationInsight®
Evaluate. Innovate. Dominate.

877.226.9950
www.transportationinsight.com
info@transportationinsight.com

About Transportation Insight

Transportation Insight is a global Enterprise Logistics Provider of customized, multi-modal supply chain services. We help manufacturers, distributors and retailers maximize profits, enhance customer service, reduce cycle times and increase supply chain visibility.

2016 Transportation Insight, LLC. All rights reserved. Ken Rev.1 6/2016