

# Disposal Risks

## *Best Practices for Mitigating Risk During IT Asset Collection*

### Beyond the Hype

Much of the hype around IT asset disposal casts a wary finger at recyclers and how they handle toxic substances found in electronics and how they handle data stored on hard drives. This article explores risks that occur well before your assets ever reach their doors—during the asset collection process.

Most current discussion around regulatory compliance in IT asset disposal has to do with complying with environmental regulations enforced by states or by the EPA. Most of those regulations affect an asset manager’s choice and management of the recycler or remarketer who will be handling the final disposition of assets. Most of the worries are about dumping in landfills, illegally exporting CRTs or other activities that occur after the assets reach the service provider’s facility.

### Compliance Leads to Risk

Data security regulations like Sarbanes Oxley and HIPAA also greatly affect governmental organizations, public companies, financial institutions, health care organizations and even retail chains with customer information stored on the computers that they may be returning at the end-of-a lease or end-of-life.

For example, the Safeguards Rule of the Gramm-Leach-Bliley Act requires financial institutions to develop an information security plan that describes how the company protects their clients’ nonpublic personal information. These plans must extend beyond company walls to include the logistics and transportation process involved in disposal.

The ownership, and therefore the risk of loss of these assets and the information stored on them do not transfer to the leasing company or the recycler until they have been successfully delivered to their facility. This is where compliance leads directly to risk management that must include the IT asset collection process.

### Key Risk Opportunities

There are several points in the IT asset collection process that present opportunities for asset or data theft or loss, or “risk opportunities.”

- The first risk opportunity occurs during the packing

process onsite – can you trust the crew and the quality of their packing? How are they recording what they’re packing?

- The next point of risk occurs when the truck pulls away with the pickup – how do you prove what they took, who they are, and where they’re going?
- The first cross-dock represents another risk opportunity – can you be sure your assets are not sitting outside or left unsecured for a period of time?
- The next cross-dock or hub represents a similar risk. Can you be sure your assets are not mixed or switched with someone else’s?
- The point of delivery or final destination is the last risk opportunity – can you be sure that what is off-loaded is complete, and what is audited is accurate?



As with most things, as soon as you try to reduce risk, you increase cost. And when you cut corners to reduce cost, you increase risk.

On one end of these extremes is the cheap and **easy** practice of having Joe’s Moving service from down the street come and pack up your computers that have customer data,

patient data or financial data on the hard drives. The packing crew throws them on pallets, shrink-wraps them and takes off. They don't record any information about what they just took. They give those three pallets to Lowball Freight Company who runs them through four warehouses to consolidate and reconsolidate the load to keep costs down. At any point, any dock worker could take or swap any asset and it could be on eBay within 24 hours. How would you know?



On the other end of the risk management spectrum is to pack up your own assets and have Brinks come and pick it up with their two armed guards to drive it in a locked and sealed truck directly to your environmental partner. It's extremely expensive, but very little risk.

**Best Practices to Mitigate Risk**

The best practices should encompass a way to try to get the best of both worlds: moderate risk at moderate cost.

First, at the onsite packing stage, these three steps are a good start:

1. Use a provider who can certify that their crew is trained on packing IT assets.
2. Make sure they record what they are packing as it's packed, preferably in digital format to avoid the mistakes of hand-written notes and manual data entry.
3. Ideally, start with a list of the asset tag numbers of the equipment to be taken so you can verify every asset packed by the onsite crew.



**Onsite Packing**

Second, build in some accountability into the pickup:

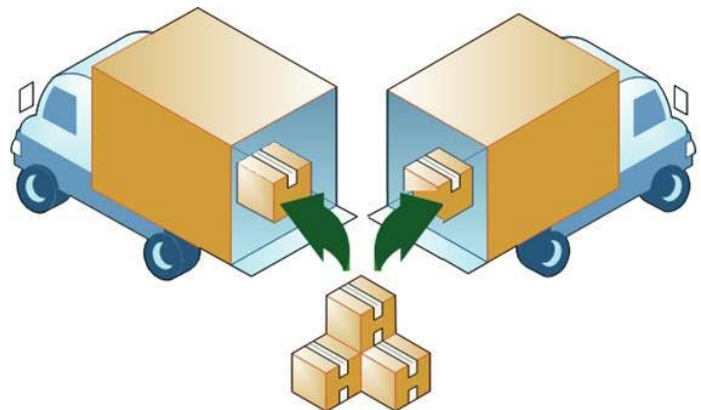
1. Make sure the same company that packs the assets also picks up—as a single event. This gets closer to “one throat to choke” if things go wrong. The more parties involved in the process, the less secure it is.
2. Require a signed Proof of Pickup that documents how many of each asset type was picked up.
3. Make sure you have the driver's name and signature on his company's manifest so you know how to follow up if you need to.
4. Make sure you verify the information about the logistics company, the driver and the asset count before signing a release of the assets.



**Pickup**

Third, insist on visibility in transit:

1. Choose a service provider that allows you to track your assets online while they are in transit.
2. Ask which cross-docks or facilities your assets will be passing through.
3. Ask about the security in place at each facility—there should be security cameras, screened personnel only, locked doors at all times and freight should never sit outside a facility unless it is in a locked truck.
4. Request that your pallets of assets be machine-wrapped at the earliest opportunity to minimize load-shifting and damage.



**Cross-docks**

Fourth, tighten the controls at the final delivery:

1. Make sure your leasing company or environmental partner documents or photographs the condition of pallets and assets on the truck before they unload upon delivery.
2. Get a Proof of Delivery from the logistics provider.
3. Make sure the Proof of Delivery matches the Proof of Pickup, and match the asset list from the pick up with audit report from the EP.



**Delivery**

Finally, just as recyclers issue a Certificate of Disposal, you should ask for get a Certificate of Collection to document every asset and every pallet picked up and delivered, as well as, and every arrival and departure along the way. This document should give you a breakdown of assets by type

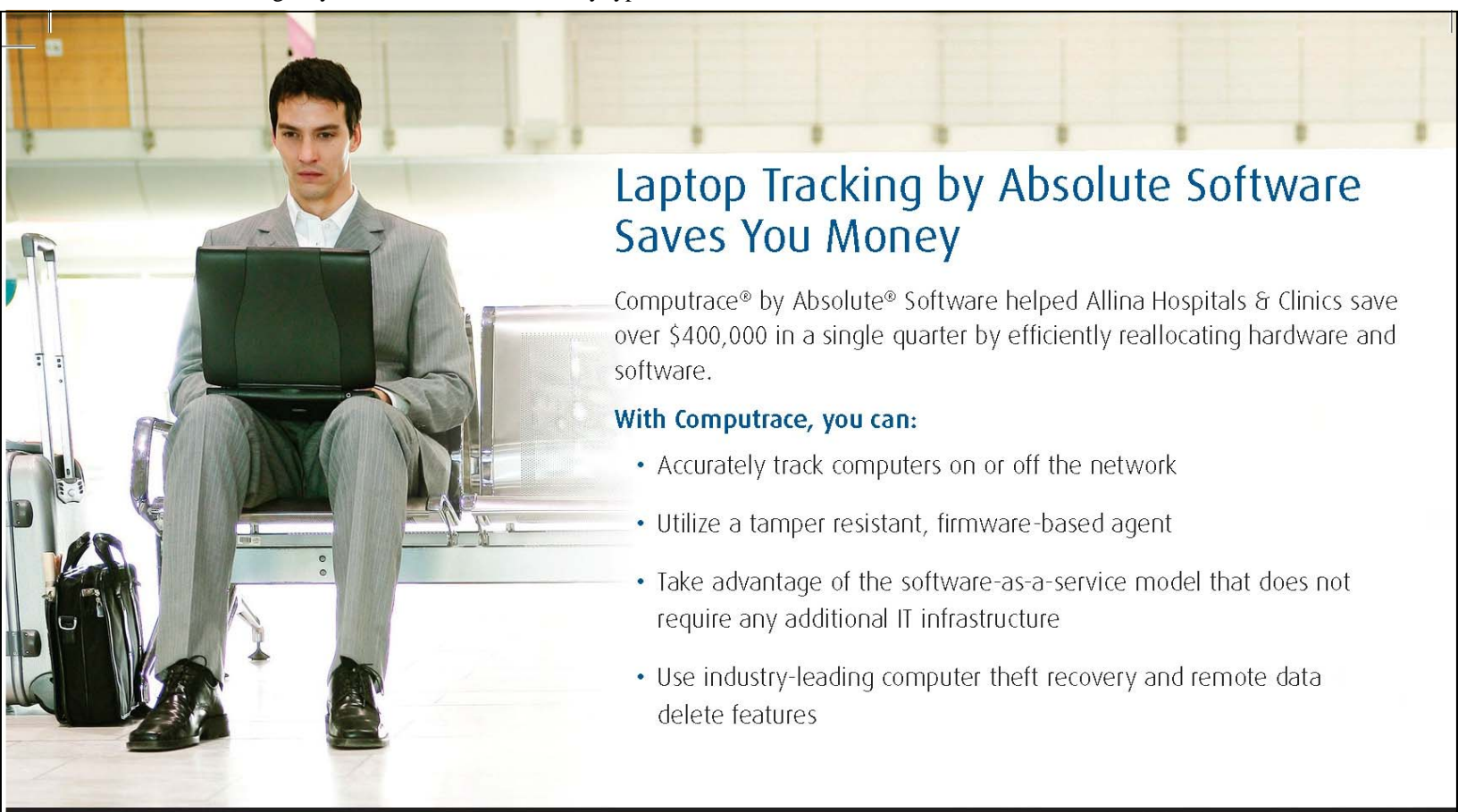
(CPU, CRT, etc.), brand, cosmetic grading, and a reconciliation of what was expected to be collected vs. what was actually collected.

The basic premise for best practices for IT asset collection



is to maximize visibility and accountability throughout the IT asset collection process. Any service provider you choose should be scrutinized for their standards on both counts and the technology they have in place to implement those standards efficiently.

**Shawn Stockman**  
*Business Development*  
 OnePak, Inc.



## Laptop Tracking by Absolute Software Saves You Money

Computrace® by Absolute® Software helped Allina Hospitals & Clinics save over \$400,000 in a single quarter by efficiently reallocating hardware and software.

### With Computrace, you can:

- Accurately track computers on or off the network
- Utilize a tamper resistant, firmware-based agent
- Take advantage of the software-as-a-service model that does not require any additional IT infrastructure
- Use industry-leading computer theft recovery and remote data delete features