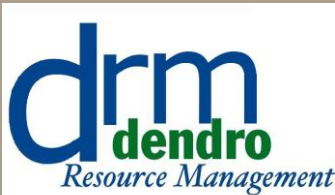


**Dendro Resource Management, Inc.**  
*provides audit, security and consulting services  
designed to raise the theft and fraud prevention stance of the timber industry.*



**In this issue:**  
**Introduction by  
Aaron:**  
How is Your Integrity?  
**Featured Article:**  
Your Best Fraud  
Prevention Efforts Include  
Your Biggest Allies: Your  
Employees  
**Issue: June 2011**



## About Us

With over 23 years' experience in the forest products industry, Dendro Resource Management, Inc. (DRM) is a leader in timber audit services. DRM is committed to supporting the integrity of the forest industry by providing independent analysis and recommendations regarding internal controls as well as actively detecting and documenting theft and fraud incidents. Customer programs can be tailored with your Company's needs in mind. With DRM you are guaranteed independence and confidentiality.

Learn more about our

## How is your integrity?

What a good headliner in a campaign to solicit employee support for fraud prevention and detection. By focusing on integrity you are not only creating an environment and internal culture that seeks the highest ethical standards, you are making the message personal. And that's right where you want it to be - up front and personal.



As we have stated in prior newsletters, people steal if three conditions are present -- the person has an immediate financial problem, there is opportunity, and the person can rationalize the theft. Therefore, since people generally steal for personal reasons, to overcome that personal response to theft requires a personal communications effort. Here's what it might sound like:

*Even the strongest structure needs a foundation. Our foundation is your integrity. There's nothing more important. When we act fairly, honestly and with respect at all times, our customers, suppliers, co-workers and stakeholders and even our competitors view us as an ethical company and will want to do business with us. However the opposite can be true as well. If we act dishonestly, unfairly and disrespectfully, our reputation suffers and so does our ability to win new business. It's not always easy. But when others decide to steal from the company, we all suffer.*

This month we'll talk about how to tap the integrity of good employees to help in your anti-fraud campaign. We'll focus on a three-legged approach: [employee education](#), [internal controls](#), and [the use of an ethics hotline](#).

**Aaron Gilland**  
DRM, Inc.

**The Best Fraud Prevention Efforts Include Your**

## products and services

[Check out our website](#)  
[About Us](#)  
[Our Services](#)

[Prior Newsletters](#)



### Quick Links and Resources

[ACFE \(Association of Certified Fraud Examiners\)](#)  
[Society of American Foresters](#)

[Optic-Solutions, Inc.](#)  
[National Federation of Independent Business](#)  
[South Carolina Forestry Association](#)

### Sample Codes of Ethics

*As follow up to our last article, here are some samples of Code of Ethics policies:*

Thanks to my colleagues at the Packaging Corporation of America for sharing their [PCA Code of Ethics](#)

The Code of Ethics for the Association of Certified Fraud Examiners is here [ACFE Code of Ethics](#)

## Biggest Allies - Your Employees

Fraud specialists and even supervisors and other management types can't be in all places at the same time. Fraud perpetrators count on that. They learn the systems and processes and even the habits that are in place and use that knowledge to work



around them. They also count on other employees either going along with them as accomplices or wanting to avoid getting involved. Not turning in a fellow employee who is stealing can be a stronger value than the stealing itself. In a way we

were taught that way. As kids, the one who tells about the bad performance of a brother or sister got in the same amount of trouble, not for doing anything wrong but because they "tattled." Those lessons carry over with us for a very long time.

To change that "tattling" mentality and help employees know

when it's important to make the tough choice to tell will take more than a brief overview of the ethics policy during the hiring process or a review during the obligatory annual meeting where everyone knows the real purpose is to get it over as quickly as possible and get signatures to prove that people came.



## Employee Training

Employee anti-fraud training programs should be conducted once a year to review the company's ethics policy as well as other issues regarding ethical behavior directly related to the company's business and culture. So you should just do it. Just go out on the internet and find a program and put your company's name on it and copy it. Right?

First of all, since you are teaching ethics, you probably don't want to just steal someone else's



copyrighted material, but let's assume you buy it legitimately. It's still best to think about your own situation before implementing an off-the-shelf program. It might be a good start but you should consider a few things first

that would help you make sure the training fits your organization and culture and really supports ethical behavior and isn't just a "check off the box activity."

Here are a few things to consider:

- Is it suitable to the size of the organization?
- Does the training include a way to report the crime in a timely manner? Does it give relevant examples of ethical decisions faced by employees in a particular job?
- Does it cultivate a company culture of ethical behavior and capture employee's hearts to want to cooperate?

The first step is to honestly evaluate your own company's attitude toward training. If you are concerned that your culture frowns on training (especially policy training) as a waste of time, then it's better to start with a smaller, targeted program that is successful and create a model for a later, wider rollout.

Think of training as any method you use to deliver information to help employees learn. In that light, training can take many forms such as class-room style seminars, on-line training, poster campaigns, supervisor team meetings and periodic newsletter articles or some hybrid approach that includes two or more avenues. Choose the communication method that works best in your company to show the seriousness of the subject as well as provide the applicable information. Consider situations specific to your organization as well. What resources do you have to develop the training? Are your employees in one place or spread out?

Is special training required for supervisors? After all, more than anyone, they need to know what is and isn't acceptable behavior to be able to support the company policies. This includes not just

legal ramifications but day-to-day ethical traps related to their particular area. Supervisors should be trained on "managing the law" topics, such as interviewing and hiring lawfully, lawful and effective discipline, avoiding wage-and-hour violations, family and medical leave, accommodations for disabled and ethnic situations and workplace violence prevention, harassment and discrimination issues. All of those areas, if handled poorly, can lead to ethical issues for the employees, the supervisor and the company.

If you are using a meeting format, require everyone to attend. Keep the content at an 8<sup>th</sup> grade level to ensure everyone "gets it." Also, consider whether some employees have issues with literacy (if they must read and sign something) or English as a second language.

Include senior executives and managers. Why?

- Sr. Executives aren't immune to fraud and in fact are in a position to steal higher amounts per incident from the company
- Managers act as models for all employees. Dishonest managers set a negative tone that will likely lead others to steal. However, honest managers set a positive image of honesty and integrity that will carry those same traits over to employees as well.
- Managers need to be very familiar with the company's ethical policies and be able to spot red flags that signal internal fraud as quickly as possible.

*What content should be included?*

It's important to not only include an overview of the company's ethics policy but to also give examples and specific guidelines for certain situations that are likely to arise. This will not only tell employees what they should do but will also tell employees what will happen if they don't follow the policy.

At the same time, avoid preaching or making threats. Since most employees are honest, this can only serve to feel like being accused when innocent which lowers morale and creates a management versus employee environment. Too hostile a message can anger employees to the point that it can actually lead to the fraud you are trying to prevent. A good education program explains how fraud and abuse cuts into company profits and, by extension, employee raises and promotions.

The program should also discuss the psychology of fraud and how otherwise honest employees have sometimes stolen from their companies. Understanding the triggers for fraud helps employees not only understand how fraudsters think but also helps set the ground work for a discussion of red flags to look for that might indicate a fraud situation.

Employees should also learn how to recognize when a fraud is occurring and how to report it. For instance, they should be suspicious of another employee's sudden change in lifestyle (without any known reasons for the change) and wonder if that can be a sign of fraud occurring. They should also know that you are looking for suspicious behavior but will investigate the situation yourself in case there is a legitimate reason for the behavior. They don't have to have positive proof of fraud before reporting it. They should know they will be taken seriously, that their involvement will be kept confidential and that the company won't bring repercussions against them for providing the information. Having a confidential and outsourced way to report suspicions is a good way for employees to know the information will be handled discretely.

Finally, after the program is in place, content should be refreshed to ensure its timeliness and accuracy. It should always reflect the latest guidelines, regulations and legislation.

Have a process in place to track when employees have completed the training modules. With that, collect feedback that ensures employees got the message and that the program is working effectively. Get feedback about how it could be improved and use that to keep the material fresh. Collect examples of issues employees face and address those as well.

### **Internal Controls**

Through well-structured, well-communicated and sound accounting and other process practices and procedures companies can make a big difference in preventing and detecting internal fraud. Employees who know what they should be doing and are diligent in following procedures will automatically establish an anti-theft system that monitors itself. The problem



comes when procedures aren't organized in a way that supports theft prevention and following them becomes lax and haphazard. Since most fraudulent activities are carried out by people we know, employees should understand that procedures are to be followed whoever is involved.

It's just good practice and it supports a discipline that becomes part of the culture - the "way we do things around here."

A critical piece of a solid, anti-theft process is to ensure there is a division of responsibilities. That means employees who perform critical jobs, especially with cash, don't handle the documentation and records of those transactions. It applies in

other areas as well. For instance, it also means that purchasers who work agreements with suppliers don't also apply the contracts into the accounting system. This is pretty much standard operating procedure in large companies but can get tricky in small companies where, at times, there is more work to go around than people to do it.



Audits should be done on a routine basis to reinforce standard practices and to deter and/or stop detected fraud as soon as possible. At the same time, audits should be conducted randomly on a surprise basis. That way, potential fraudsters can't anticipate your schedule and hide their handiwork.

Companies can do this either through a subcommittee of the board of directors, the internal audit team or an outside consulting company that specializes in the timber industry. It's important to have an outside party conducting the audit to ensure the integrity of the process. This will serve as a watchdog over all levels of the organization.

Auditors should:

- compare one year to the next to find obvious differences and seek explanations for those
- review operational policies and test to those policies against actual "field processes"
- check inventory levels and the frequency of adjustments to inventory to verify the inventory process.
- check addresses of suspicious vendors against a list of employee home addresses
- Examine checkbook and escrow account management for possible red flags

Depending on the company, there are many other audit approaches, too numerous to list here.

Successful audits are grounded on solid anti-theft procedures and dependent on employees being diligent about following them. When something is out of the ordinary, employees will catch that something isn't being done right and that will raise flags. Otherwise, the process itself will limit the fraudster's opportunity and, in many cases, prevent problems in the first place. Remember that one leg of the fraud triangle is that the person sees an opportunity. If the risk of getting caught is too great, they won't even try it.

### **Hot lines**

Finally, companies should have some mechanism where

employees, vendors and contractors can anonymously report possible red flags or fraudulent actions discretely. As we said before, employees are reluctant to report the behaviors of their co-workers. They often see catching thieves as the work of management or security and not theirs. However, if they become angry or upset enough about what they see or think they see going on, they will call in, if they have an avenue to do so.

Just knowing that this is available raises the fraudster's fear of being caught. They can avoid the supervisor or manager's watchful eye but will often have a hard time keeping their actions from fellow co-workers, at least for long periods of time.



To be effective, companies have to publicize the hot line, its availability and its purpose. Remind employees that it's ok to provide name and contact information but isn't required and in most cases not even necessary. Ensure the system is confidential and easy to use. There are a variety of ways to do that including posters, wallet-sized cards, coffee mugs, cafeteria tent cards and periodic communications reminders in employee newsletters and other information avenues. Be creative in coming up with ways to remind employees of the hot line and make the number easily available. If you can, utilize a third party provider to manage the hotline. They will more likely do a better job of keeping track of calls and some can even provide 24 hour service with a live representative on the other end of the line. Since there can be long periods with no activity, if managers are handling the line, it's possible that they lose the discipline of checking the system for messages regularly as long periods of silence prevent them from checking daily and they get caught up in daily activities.

These hotlines should be emphasized as just another avenue of communication, and reinforce that the supervisor is still the primary contact and maintains an open door for you to discuss any ethical concerns. The system isn't meant to be a substitute for communication between employees and their bosses. If the system is run by an outside firm, it will be difficult if not impossible for them to answer specific local questions about the operation. At the same time, if employee's have already tried their supervisor or are concerned their supervisor's involvement is jeopardized, the hot line is the place to go.

Once established, a hotline can serve to collect employee information about much more than theft and fraud issues.

Encourage employees to report the following types of situations:

- On-the-job drug or alcohol abuse
- Harassment or discrimination

- Theft or property damage
- Poor workmanship or inappropriate "shortcuts"
- Health, safety and environmental issues
- Violations of company policies or procedures
- Any other violations of applicable laws and regulations.

**Conclusion**

There you go - three areas where you can use employees to help you manage your fraud prevention program. Are you tapping your internal resources or trying to catch perpetrators on your own? How is the integrity of your employees? How is yours?