

# DEALERSHIP

A SERVICE OF

# INSIDER

fall  
09



HENDERSON HUTCHERSON  
& MCCULLOUGH, PLLC  
CERTIFIED PUBLIC ACCOUNTANTS

## EMPLOYEE FRAUD

---

### Many Scams Start In the Finance Department

Employee fraud — sadly, it can strike any kind of business, including auto dealerships, and it costs consumers and business owners millions of dollars each year.

Employees take wrong turns, either for their own profit or to win approval by bumping up the dealership's bottom line. In auto dealerships, fraudulent activity often revolves around the financing department and its relationship with customers. Sometimes a salesperson is part of the scam.

You can protect against fraud and, in the process, protect your dealership's reputation — and your industry's. But you've got to know how to recognize the beast before you can hunt it. Here are some common employee scams involving the financing phase of sales.

#### PRESENTING A BOGUS CREDIT SCORE

In this fraud, a financing department employee lies to the customer about his or her credit score, saying it's lower than it really is. The employee then charges the customer a higher interest rate, increasing the dealership's income from the sale.

Crooked employees try this on customers who won't be too surprised to hear they're having financing problems. Most consumers with strong credit ratings would know they were being duped.

One way to prevent this scam — and, indeed, most financing-related scams — is for a finance manager to review all customer agreements. If a customer's credit score doesn't mesh with the interest rate being charged, foul play could be to blame.

Just be sure to rotate reviewing duties among several

finance managers. If you don't have more than one, randomly review customer agreements yourself on occasion.

#### FAKING FINANCING APPROVAL

This scam involves telling the customer that he or she has been approved for financing, delivering the vehicle and letting the customer drive it for a few weeks. But then the other shoe drops: A financing department employee calls back to say that the loan fell through and, to keep the vehicle, the customer must pay a premium and a higher monthly payment.

Again, crooked employees usually practice this rip-off on customers with poor credit, who they assume feel shaky about their credit worthiness. The employee knows the real payment amount and the interest rate offered by the financing institution before delivering the car. But he or she assumes that, after driving the vehicle for a time, the customer will develop a certain comfort level and agree to pay more to keep it.

To catch employees doing this, watch your contract in transit schedule to see if any deals are taking too long to be funded. You also can send out customer satisfaction surveys and read any responses received carefully. If you notice several buyers — or even one — complaining that their monthly payment went up unexpectedly, investigate further.

#### PADDING TOTALS

In this fraud, a finance department employee includes items in the vehicle price that the customer didn't agree to, such as destination fees, and, most frequently, warranty costs.

The salesperson quotes a price that doesn't include the warranty fee, and then gives the customer the monthly payment amount that does include it — without getting the customer's consent.

If the customer questions the warranty, the salesperson may say it's required in order to lock in a certain interest rate. This is false: The interest rate depends on only the customer's credit history.

Once again, regular, unannounced reviews of customer agreements can turn up scams such as this one. In addition, be sure to inform finance department employees of the consequences of fraudulent behavior. Clearly state that you have a no-tolerance policy toward wrongdoings and remind them that you'll occasionally, and without warning, review their work for accuracy.

#### STAYING VIGILANT

To prevent, or at least curtail fraud, dealers must stay vigilant. As your employees make sales and your dealership makes money, don't assume all is well; frequently check up on what's really going on. Make sure you're doing enough to protect your dealership's image and standing in the community, which is, after all, your most precious asset.

## HOW MUCH IS FRAUD COSTING YOUR DEALERSHIP?

Crooked employees and dealers who commit fraud may be making a few extra dollars per vehicle, but they're losing a lot more.

After all, most dealership revenue comes from loyal repeat customers. Defrauding customers costs a dealership potential repeat business, such as additional car sales and service. And that's not to mention the threat of legal action and criminal prosecution.

Plus, you could be losing out on new customers. Before buying cars, many people look at a dealership's reviews by past customers. If your employees are scamming customers, the public may know about it before you do.

For further information, please contact Henderson Hutcherson & McCullough, PLLC today.

## INTERNAL CONTROL CONCERNS

**Trillions of dollars** of EFT and ACH transactions are consummated daily throughout the world, with these transactions becoming more and more voluminous in dealerships. Improper implementation of internal controls as well as a lack of supervision and review of actual EFT and ACH transactions could potentially result in financial disaster for your dealership from fraudulent activity. Do you know who is transferring cash in your dealership and where it is going? Who is reviewing such transactions and internal controls? Are your internal controls adequate and properly functioning in respect to cash transfers?

The extent of application of internal controls, supervision, and review of EFT and ACH transactions will vary in complexity from business to business. Therefore, a simple checklist or a "cookie cutter" approach in addressing the issue may be considered inadequate. Although a very incomplete list, we have provided a few thought provoking items relating to cash transfer outflows:

#### SYSTEM SECURITY AND ACCESS CONTROL IN PROCESSING EFT AND ACH CASH TRANSFERS

- Are the computer and related programs located in a secure environment and locked when not in use?
- Are the computer programs relating to cash transfers accessible in any manner by unauthorized users (i.e., from other terminals in a network environment, internet or the physical workstation)?
- Are up-to-date lists of users and their levels of access maintained?
- Does appropriate management adequately supervise the physical security of the computers that in any manner have access to programs related to cash transfers?
- Is it possible that computer access passwords and other vital information have been leaked, intentionally or not, to others? Are passwords and other vital access information changed periodically? How is this documented?
- Are system records maintained to document logon attempts/session paths, etc. and are they reviewed by appropriate management? Does the system maintain log-on violation records?
- Is the specific computer or terminal validated and documented by the system upon attempted log-on?
- Is input documentation reviewed and approved independently of the cash transfer process? How

many approvals are required and how are they documented?

- Are prospective employees that will be involved in the cash transfers properly “screened”? Are they adequately bonded?
- Do processing periods ever become prolonged? Are employees leaving the computer during the transmission process?
- How are computer hardware and software problems documented related to the cash transfers?

#### **Who is supervising compliance with internal controls relating to these matters?**

#### **INTERNAL CONTROL OVER PROCESSING EFT AND ACH CASH TRANSFERS**

- Is there a pre-approved listing of vendor numbers and bank account numbers for which designated cash transfers can be made to/from?
- Which employees are permitted to perform what type(s) of cash transfers? How is this monitored? Are there pre-approved dollar limitations?
- Is cash reconciled by an individual independent of having access to perform cash transfers?
- Is the cash reconciliation or review completed from internet or computer generated statements that could have been easily manipulated prior to being reviewed?
- Does the cash reconciliation process include a detailed review of vendors, bank account numbers and other references relating to the cash transfers? Is supporting documentation reviewed?
- What is your exposure that unauthorized transactions are occurring with your authorized vendors (i.e., an employee paying a personal debt with an identical vendor)?
- What is your exposure that “innocent looking” payroll tax deposits made via cash transfers are crediting unauthorized amounts of federal income tax to an employee’s withholding account?
- Are recurring cash transfers reviewed to determine the on-going propriety of the amount and the authorization of the expenditure?

These are only a few of the many internal control issues relating to the controlling and processing of EFT and ACH transactions. Need a check-up? Contact Henderson Hutcherson & McCullough, PLLC today.

## **TAX TIP: PONZI SCHEME GUIDANCE**

The IRS has issued guidance to assist taxpayers who are victims of losses from Ponzi-type investment schemes. The IRS guidance is not specific to any particular case. The first item is a revenue ruling that clarifies the income tax law governing the treatment of losses in such schemes. The second is a revenue procedure that provides a safe-harbor method of computing and reporting the losses.

The revenue ruling determines the amount and timing of losses from these schemes as factually difficult and dependent on the prospect of recovering the lost money (which may not become known for several years).

The revenue procedure simplifies compliance for taxpayers (and administration for the IRS) by providing a safe-harbor means of determining the year in which the loss is deemed to occur and a simplified means of computing the amount of the loss.

The revenue ruling sets forth the formal legal position of the IRS and Treasury Department:

- The investor is entitled to a theft loss, which is not a capital loss. In other words, a theft loss from a Ponzi-type investment scheme is not subject to the normal limits on losses from investments, which typically limit the loss deduction to \$3,000 per year when it exceeds capital gains from investments.
- The revenue ruling clarifies that “investment” theft losses are not subject to limitations that are applicable to “personal” casualty and theft losses. The loss is deductible as an itemized deduction, but is not subject to the 10 percent of AGI reduction or the \$100 reduction that applies to many casualty and theft loss deductions.
- The theft loss is deductible in the year the fraud is discovered, except to the extent there is a claim with a reasonable prospect of recovery. Determining the year of discovery and applying the “reasonable prospect of recovery” test to any particular theft is highly fact-intensive and

can be the source of controversy. The revenue procedure accompanying this revenue ruling provides a safe-harbor approach that the IRS will accept for reporting Ponzi-type theft losses.

- The amount of the theft loss includes the investor's unrecovered investment – including income as reported in past years. Some taxpayers have argued that they should be permitted to amend tax returns for years prior to the discovery of the theft to exclude the phantom income and receive a refund of tax in those years. The revenue ruling does not address this argument, and the safe-harbor revenue procedure is conditioned on taxpayers not amending prior year returns.
- A theft loss deduction that creates a net operating loss for the taxpayer can be carried back and forward according to the timeframes prescribed by law to generate a refund of taxes paid in other taxable years.

The revenue procedure provides two simple assumptions that taxpayers may use to report their losses:

Deemed theft loss.

- The revenue procedure provides that the IRS will deem the loss to be the result of theft if: (1) the promoter was charged under state or federal law with the commission of fraud, embezzlement or

a similar crime that would meet the definition of theft; or (2) the promoter was the subject of a state or federal criminal complaint alleging the commission of such a crime, and (3) either there was some evidence of an admission of guilt by the promoter or a trustee was appointed to freeze the assets of the scheme.

Safe harbor prospect of recovery. Once theft is discovered, it often is difficult to establish the investor's prospect of recovery. Prospect of recovery is important because it limits the amount of the investor's theft loss deduction.

- The revenue procedure generally permits taxpayers to deduct in the year of discovery 95 percent of their net investment less the amount of any actual recovery in the year of discovery and the amount of any recovery expected from private or other insurance, such as that provided by the Securities Investor Protection Corporation (SIPC). A special rule applies to investors who are suing persons other than the promoter. These investors compute their deduction by substituting "75 percent" for "95 percent" in the formula above.

If you are involved in a Ponzi type loss you should discuss its deductibility with Henderson Hutcherson & McCullough PLLC.

## CALL THE DEALERSHIP SPECIALISTS AT HENDERSON HUTCHERSON & MCCULLOUGH, PLLC

Randall Hebert, MBA, CPA, CVA  
423.702.8145  
rhebert@hmcpcas.com

Travis M. Horton, MBA, CPA  
423.702.7275  
thorton@hmcpcas.com

Chet Logan, CPA  
423.702.7262  
clogan@hmcpcas.com



HENDERSON HUTCHERSON & MCCULLOUGH, PLLC  
CERTIFIED PUBLIC ACCOUNTANTS

1200 MARKET STREET | CHATTANOOGA, TN | 423.756.7771 | HHMCPAS.COM