HEADLIGHTS

A PUBLICATION
OF THE AutoCPAGroup

WWW.AUTOCPA.COM
1-800-4AUTOCPA

IRS GUIDANCE ON FACILITY IMAGE UPGRADE PROGRAMS

Manufacturers commonly require dealers to update their dealership facilities under facility image upgrade programs. To entice dealers, some manufacturers may offer cash incentives in many different forms to assist with project costs.

The IRS recently considered specific situations for three different facility image upgrade programs. In each case, it concluded that payments received by dealerships for these programs qualify as taxable income.

John Hayes, CPA
Maloney + Novotny, LLC

On May 9, 2014, the Office of Chief Counsel of the IRS issued General Legal Advice Memorandum (GLAM) 2014-004. This GLAM is consistent with previous IRS positions on this subject. The IRS considered the following arguments to possibly exclude the facility image upgrade payments from taxable income:

1 Facility image upgrade payments should be considered nonshareholder capital contributions.

2 The basis in the related constructed assets should be reduced by the amount of facility image upgrade payments received.

3 Payments should be considered as a purchase price adjustment to vehicles acquired from the factory.

Nonshareholder contributions

Tax rules governing nonshareholder contributions are by intention very restrictive. Among other requirements, the contribution or transfer must be made to benefit the general community rather than the transferor directly. Because factory payments are intended not only to upgrade the dealership facility but to improve sales and

please turn the page ☞

customer service for the benefit of both the dealership and the manufacturer, the IRS concluded this requirement is not met.

Reduction of basis in the property

The income tax basis of acquired property starts with its cost and is increased by the cost of any capital improvements. Furthermore, gross income is broadly defined to include "all income from whatever source derived" over which the taxpayer has control.

The dealership, not the manufacturer, owns the property and hires the contractors, so the IRS reasoned that even though manufacturer's payments may be used to defray the project's costs, such payments are under dealership control. Thus, they are considered gross income and may not reduce the basis of the property or its improvements.

Purchase price adjustment to vehicles

For each facility image upgrade program, the payments' primary purpose is to provide an incentive for the dealership to upgrade its facility, not to reduce the new vehicles' purchase price. That brings the payments under the tax law's broad definition of gross income as "all income from whatever source derived."

A GLAM is considered documented legal advice, signed by executives in the National Office of the Office of Chief Counsel and issued to IRS personnel to help them administer their programs by providing authoritative legal opinions on certain matters. A GLAM cannot be used or cited as precedent. Please consult your nearest AutoCPAGroup member with any questions you may have about this subject matter. ✍

INTERNET ADVERTISING

Carl Woodward, CPA
Woodward & Associates, Inc.

A portion of most dealers' advertising budget goes to the Internet, including dealership websites and third-party referral sites. Of the over 200 dealers our firm serves, the average gross advertising expense is $350 per new and used retail vehicle sold. If measured only on a new-vehicle basis, this computes to approximately $600 per new retail unit sold and compares with the 2013 NADA national number of $612 per new retail vehicle.

With few exceptions, dealers don't sell in total more vehicles because they spend some of their advertising dollars on the Internet. We find dealers selling a few vehicles, such as specialty vehicles, out of their market area, which could be a result of Internet advertising. All dealers lose some sales to dealers out of their area due to the Internet, but that number is difficult to quantify.

Dealers can identify which vehicles are being sold via Internet advertising by using a process that identifies if and where the customer found the vehicle or your dealership on the Internet. Have either your sales associates or your finance and insurance (F&I) department ask customers how they found you and the vehicle they are purchasing. If customers answer, "The Internet," ask how they searched and the keywords they used. This information can help determine if your Internet ads include keywords that consumers might use to search. In addition to keeping better track of customers coming to you from the Internet, have either your sales department or back office track the results, so a monthly report can be provided to your managers and those working on your website. If you use a check-off sheet for your deals, make this information one of the check-offs.

A reasonable percentage of the public looks for vehicles on dealer and third-party websites. For many customers, websites are like a sales brochure. List most used vehicles, along with some of your new vehicles, on your website. Price some of the used vehicles to include monthly payments,

and make them competitive with local dealers' prices for the same vehicle.

Dealerships sometimes delegate a select group of employees to respond to Internet inquiries; others direct these to their regular salespeople. Decide which works best for the way you operate. Always respond quickly (within an hour or less) and make sure the responding employees are Internet savvy.

In summary, try to identify those vehicles sold via Internet advertising, so you have some basis to determine how much to spend and which Internet services to use. This information will also assist you with your Internet ad content. Contact an AutoCPAGroup member to discuss this further. ✍

UNDERSTANDING CYBERSECURITY THREATS

William Schmidt, CISA, CISSP, PCIP
Boyer & Ritter, LLC

Computer security breaches have increased sharply during the past several years, with global losses for cybercrime reaching as high as $400 billion in 2013. Understanding the types of data targeted by cybercriminals can help a dealer make a plan to reduce the risk of cybertheft.

Primary targets for cybercriminals include credit card numbers, commercial bank account numbers, bank website passwords and confidential information (Social Security numbers, driver's license numbers, etc.) that can be used for identity theft. These have direct value when sold on the black market.

Credit card numbers can be traded and sold on so-called carder forums. These sites often connect criminals to services that allow them to purchase stolen cards, test the cards' validity and order imprinted fraudulent cards. These cards are usually used to make a single large-ticket purchase and then discarded.

Business bank account Internet passwords can be stolen by a "corporate account takeover" whereby hackers log on to your corporate bank account after stealing your passwords. Once hackers have access, they send wire transfers or Automated Clearing House (ACH) transactions to other fraudulent accounts and ultimately try to transfer the funds offshore. This can empty a business's bank account in seconds and may not be reversible.

Cybersecurity breaches usually start with malware (viruses, trojans, etc.) delivered through e-mail, a hacked website or infected devices such as USB flash drives. E-mail filtering and antivirus software can block some malware infections, but Symantec, one of the largest antivirus software companies, recently conceded that antivirus software is only 45% effective at best.

Once malware is on your network, it automatically spreads and allows hackers to access the infected system. The attacker could then search the company's network for confidential data, send out spam e-mails, launch a denial-of-service attack or install software to collect financial data. Some malware can encrypt and lock your network files and demand a ransom for their release.

The right combination of security controls can greatly reduce the risk of a successful cybercrime occurrence. Consider the following precautions:

✔ Have written computer security policies for employees.

✔ Conduct an annual computer security scan, and train employees to conduct their own scans.

✔ For business banking activities, use a separate, dedicated computer that is not permitted Internet access (other than to the bank's website) and may not open e-mails or work on other files.

please turn the page ☞

UNDERSTANDING CYBERSECURITY THREATS

(continued from page 3)

✔ Run antivirus software on all computer systems.

✔ Patch software as soon as possible after security updates are released.

✔ Perform a risk assessment to identify areas of exposure and the current level of protection.

✔ Build an incident response plan to deal with a security breach if it occurs.

Understanding risks and countermeasures minimizes the chances that your dealership will wind up with a data breach and liability for ensuing financial losses. Contact an **AutoCPAGroup** member to discuss this further. ✍