PAUL H. BURGESS, ATTORNEY-C.P.A.

525 SOUTH MAIN, SUITE 800/TULSA, OKLAHOMA 74103-4511 (918) 599-7755 VOL. 36 JULY 2014

Tax & Financial Newsletter

The American Association of Attorney–Certified Public Accountants (AAA-CPA) celebrates its 50th Anniversary this year. This July, the association held its annual meeting and education conference in Huntington Beach, CA. This Newsletter highlights some tax, accounting, and business topics analyzed in 19 hours of educational seminars. This Newsletter's topics start with a few interesting accounting facts regarding Hollywood movie productions. The next section introduces the five major doctrines the IRS considers to determine if a tax strategy is impermissible tax evasion or perhaps allowable tax avoidance. The Newsletter concludes with a 14-point checklist on how a business can reduce the probability of being hacked. First, some history of the AAA-CPA.

AAA-CPA & the U.S. Supreme Court

The association organized in 1964 to promote the rights of individuals who held both accounting and law licenses. Only 20 years ago, professionals who were dually licensed could have their legal and/or accounting licenses revoked for merely advertising they were Attorney/CPAs. It was not until 1994 in a commercial free speech case that the U.S. Supreme Court unanimously held that an Attorney/CPA could hold themselves out to the public that they are both. (*Ibanez v. State of Florida Board of Accountancy)* Ms. Ibanez is a member of the AAA-CPA.

Hollywood Movie Revenue Sources

1. The Box Office results are reported every Monday morning. The box office gross is the total of all ticket sales collected by movie theaters. The film owner, typically a studio, receives about 50% of the reported box office. The movie theater, distributors, etc., receive the other half.

2. There is a fairly consistent correlation between a film's performance at the box office and the DVD/Video-On-Demand (VOD) sales. Historically, DVD/VOD revenues are approximately 60% of the box office. However, the 60% is decreasing as DVD sales have been declining and VOD revenues have not kept up with the pace of the DVD decline.

3. Movie sales to the Big 4 network televisions are infrequent today as theatrical films are rarely on ABC, NBC, CBS, or FOX. Film sales for television are typically to premium cable networks like HBO, Showtime, and Starz, or Pay TV. The studio's revenue from a film on Pay TV ranges from $2.5 million to $20 million. The pricing is dependent upon many factors, including box office results. The pricing can be misleading because many times the studio sells to its own Pay TV network. Therefore, there is pressure for a studio to sell its own film to itself at a high price to justify higher subscription fees for its Pay TV.

4. The next important television source from films is from free/basic cable television networks. The networks bid for films typically based on when they can air the films. It is common for a major film to be pre-sold for fifteen years with each of the cable networks rotating the time slot. A major release on free/basic cable brings into the studio $20 million to $30 million over several years.

5. Foreign income is an increasingly significant revenue component of a film because movie theater construction is booming throughout the world. Recently, worldwide box office revenues have shifted to two-thirds foreign and one-third domestic allocation for worldwide releases. Only certain U.S. films are conducive to releasing worldwide. U.S. action films do well overseas, but U.S. comedies and historical films do not. U.S. sitcoms rarely generate international sales beyond English-speaking countries. One-hour dramas, game shows, and reality shows sell much better.

6. Ancillary income from merchandise, theme park rights, books (in all formats), music, character, and other income is usually about 1% to 2% of gross income. Ancillary income can earn millions for a successful project and even billions for a studio.

How much does the typical star keep from the millions they earn?

Studios, networks, and producers almost always call the "agent" first. An actor finds work through an agent. Agents then negotiate the compensation terms and other aspects of the deal. Agents typically get 10% of the income earned by the actor.

Many times, actors have personal managers as well. Personal managers assist their clients on both personal and business matters and serve to help shape the actor's image, directing their career through projects they choose, helping secure endorsements, and increasingly playing an integral role in the financing and production of a film. Personal managers charge from 10% to 15% of an entertainer's income.

Then there are "talent layers" who represent producers, directors, writers, and actors. As you would expect, talent lawyers draft the contracts and are involved in the negotiations. Talent lawyers usually charge 5% of the entertainer's income.

Entertainers also have a business manager. A business manager is a specialized accountant. They collect the entertainer's income, pay all of their bills, prepare income tax returns, and advise on all aspects of financial life, such as major purchases, insurance, estate, and family wealth matters. Business managers are paid 2.5% to 5% of the entertainer's income.

Thus, the entourage of professional advisors receives approximately 30% of an entertainer's income. An actor will pay another 30% to 40% for overhead and taxes and net about a third of their gross income for houses, cars, jewelry, art, and everything else you read about in People magazine.

The above film and actor information is summarized from Harvey Gettleson's, Esq., C.P.A. presentation and materials at the AAA-CPA Summer 2014 education seminar.

Tax Avoidance vs. Tax Evasion

Taxpayers are legally entitled to choose the most efficient tax structure for their business dealings. Nevertheless, a transaction's tax structure must comply with all of the tax laws to avoid the IRS asserting "tax evasion." There are five tests the IRS considers when determining if a transaction's or investment's tax structure is potentially tax evasion as opposed to possibly allowable tax avoidance: (1) does the transaction have Economic Substance? (2) does a legitimate Business Purpose exist? (3) can the deal pass the Sham Transaction test? (4) does the transaction have the appropriate Substance over Form? (5) does it violate the Step Transaction guidelines? The five tests overlap in many aspects and are traced back to the U.S. Supreme Court's holding in *Gregory v. Helvering* (1935).

<u>Economic Substance</u>. The doctrine has been codified in the Internal Revenue Code in a two-prong test: (a) the transaction must change, in a meaningful way, the taxpayer's economic position apart from the federal income tax benefits; and (b) the taxpayer must have a substantial business purpose. If the transaction meets the Economic Substance test, it is difficult for the government to recast it as tax evasion, but the transaction still has to pass the four other tests.

<u>Business Purpose Test</u>. The Business Purpose Test is also a two-prong analysis: (a) the transaction or acquisition has to be motivated based on a non-tax business purpose; and (b) the *method* utilized for the

deal has to be motivated by a non-tax business purpose.

Sham Transaction. The Sham Transaction doctrine is "judge-made law." It will deny favorable tax treatment when a taxpayer attempts to disguise a transaction to make it appear to be something that, in reality, it is not. A "sham" is not motivated by a legitimate business purpose other than its anticipated tax benefits because there is no reasonable expectation of profit.

Substance Over Form. The Substance Over Form doctrine is similar to a sham transaction. Essentially, the tax benefits associated with a transaction must be determined from the economic substance of the transaction and not the particular form utilized by the taxpayer. The government frequently targets taxpayers who have purposely mischaracterized a transaction through its form in order to derive beneficial tax treatment. Sometimes favorable capital gains reporting, or a "tax-free transaction," can be suspect and the IRS will assert the substance of the transaction is ordinary income or a taxable gain.

Step Transaction. A Step Transaction analysis begins with substance over form. The doctrine collapses a series of separate steps into a single transaction in order for the government to obtain a clear picture of what the separate steps are accomplishing in substance. Essentially the tax treatment is not allowed even though each independent step appears allowable. The time between each step is considered, but it is not dispositive. Of course the longer the time intervals between the steps, the more favorable it is for the taxpayer.

The courts have generally utilized three "step testing" methods. First, the *binding commitment test*. If step #1 is made, and steps #2, #3 and so forth are required, then it is probably a step transaction that will be collapsed. Second, the *interdependence test* focuses on the relationship between the individual steps. For example, if step #1 is dependent on the completion of subsequent steps, the step transaction doctrine likely has been violated. Third, the *end result test*. The end result test is used when it is clear that a planned tax result is achieved via a series of related transactions that could not be achieved via a single transaction. The end result test focuses on intent. Thus, if the intent to reduce taxes is absent, the steps just may be respected and the transaction will not be considered impermissible tax evasion.

The above has been primarily summarized from David Klasing's, Esq., C.P.A. presentation and materials at the AAA-CPA Summer 2014 education seminar.

Reducing Your Risk From Hackers 14 Point Checklist

Typically, hackers send a phishing email to random staff. When a victim clicks on the link, the computer is infected with a virus that monitors activity and captures passwords, files, and other information. You can protect your company by using this 14-point check.

√ **USE STRONG POLICIES AND PROCEDURES**
Make sure all employees sign an Acceptable Use Policy that includes security-related items. Create a comprehensive cyber security policy framework. Review and revise all policies annually.

√ **LIMIT YOUR STAFF MEMBERS' PRIVILEGES**
Limit what staff can do on their desktop. Make sure they cannot change the system configuration or install any software without prior approval.

√ **DEPLOY EFFECTIVE ANTIVIRUS**
Install antivirus software on ALL computers. Use it and keep it up-to-date. Check at least monthly to make sure it is running properly on all systems.

√ **TRAIN YOUR STAFF**
Train all employees to report suspicious activity to a designated company contact. Provide social engineering awareness training at least once a year; especially for employees with access to sensitive information or finances.

√ **PROTECT AGAINST SPAM**
Make sure all spam filters are working and kept up-to-date.

√ **ENCRYPT, ENCRYPT, ENCRYPT**
Prevent unauthorized access to your data. Encrypt hard drives, backups, sensitive files and email.

√ **UPDATE YOUR SOFTWARE**
Keep your software up-to-date with the latest patches at all times. New software also includes new security 'fixes' that can save you money and hassles.

√ **KNOW WHERE YOUR DATA IS STORED**
Keep track of phones, tablets, and USBs. Decide whether staff may access and store data on home computers and other personal devices.

√ **VET VENDORS AND THIRD PARTIES**
Know your vendors' security practices. Review their security test results annually. Understand their terms of service, data ownership provisions, and breach response practices. Ask for references and check them.

√ **RESPOND QUICKLY AND APPROPRIATELY**
If you suspect that a computer with access to confidential information has been infected, unplug the network cable immediately and notify your designated IT contact.

√ **BACKUP**
Backup your data. Test your backups. Store a copy securely offsite. Repeat.

√ **KEEP YOUR EYE ON THE CLOUDS**
Understand the terms of service and privacy policy of cloud-based services. Find out where your data is physically located, who has access and what security measures exist.

√ **GET INSURANCE**
Talk to your insurance provider about options for coverage in the event of a network infection or hacked corporate computer.

√ **TEST YOUR SECURITY**
Check your internal and internet-facing network security at least annually. Get a vulnerability assessment or penetration test to make sure your network is secure.

The above introduction and checklist is wholly from Sherri Davidoff's, GCFA, GPEN, of LMG Security presentation and materials at the AAA-CPA Summer 2014 education seminar.

The statements contained herein are basic overviews of the covered subjects. Most of these provisions have special rules, conditions, and exceptions. Further, the opinions of the author contained herein are to be viewed as opinions only. Please call 918-599-7755 to see how you can make the most of these suggestions, or if you need help arranging your personal and business affairs to pay as little tax as possible.

This newsletter is a publication of Paul H. Burgess, Inc. Mr. Burgess is a member of the American Association of Attorney-Certified Public Accountants. Attorney/CPAs provide special and unique services to their clients as a result of their legal and financial training. An Attorney/CPA can analyze the financial statements, tax returns, and other information presented that considers how they fit in with the available legal, tax, and other considerations. As such, when you have legal matters that involve financial decisions, or vice versa, an Attorney/CPA may offer the best solution.