

POSSIBILITIES

INSIGHTS FOR BUSINESSES & INDIVIDUALS

OCTOBER 2011



Tax Reform

Boosting Economic Confidence

It is hard to imagine, but over the last few months, we have lived through the U.S. debt ceiling crisis, the first down grading of the U.S. government credit rating, the continuing European debt crisis and the ongoing, seemingly endless, discussion of another recession. It is no wonder our economic confidence level is low or perhaps nonexistent.

A General Overhaul

A result of the disorder and discussion we have seen in Washington, D.C., may be something that has eluded Congress since 1986—a major general tax reform. However, there are still many obstacles to overcome before any general overhaul of the tax code can be accomplished.

In the midst of the debt ceiling debate, tax reform suggestions were being offered up by both democrats and republicans. However, with the House of Representatives currently controlled by the Republicans and the Senate currently controlled by the Democrats, it is unlikely they will find the idea of any major tax reform measure offered by the opposite party worthy enough to pass both chambers.

Instead of the available 540 representatives and senators making the decision of potential tax reform, it will be placed in the hands of the 12 members of the Joint Select Committee established in the Budget Control Act of 2011. The Joint Select Committee has been formed to deal with U.S. debt reduction, which many observers, but not all, believe offers the opportunity to suggest major tax changes with the requirement that Congress take action by the end of December.

What tax items should be reformed and when would the reform take effect?

The end of 2011 is in sight, and the IRS is hoping for no major changes to any 2011 tax law. The cost and time required to reprogram their systems for filing 2011 tax returns becomes more difficult when changes are made late in the year.

We are also moving rapidly into the next major election season, and no democrats or republicans up for reelection want to be on the leading edge of tax reform. And with the

Tax Reform—continued on page 7

Instead of the available 540 representatives and senators making the decision of potential tax reform, it will be placed in the hands of the 12 members of the Joint Select Committee ...



inside

2

Effects of the Economy

3

2011-2012 Business Tax Planning
Summary of Tax Depreciation
Incentives

4

Spear Phishing: A New Danger
for Small Businesses

5

Got Mobile?
Learn How to Properly Protect
Your Business and Personal Data

6

Medicare:
An Awareness Discussion

7

A Blue Ribbon Panel Update
Where Is Private Company
Accounting Going?

EideBailly®

CPAs & BUSINESS ADVISORS

Areas to Consider in an Uncertain Economy

Given today's uncertain political and economic climate, it is important to pay close attention to your finances and business assets. Here are a few topics to consider.

Roth IRA Update: Recharacterize and Reconvert

Ken Wolff, CPA - Partner

In recent years, tax laws have provided significant changes to the rules surrounding Roth IRAs. Effective after 2009, the ability to make a conversion to a Roth IRA was opened to all taxpayers irrespective of their income level. In addition, 2010 Roth conversions allowed the taxpayer to be taxed on the entire conversion in 2010, or defer the taxability of the conversion equally in 2011 and 2012.

Recharacterize

As we move past 2010, current and future Roth IRA conversions will be reported as income in the year it takes place. Therefore, it is a good time to review some of the tax law provisions that provide the investor some additional flexibility regarding these conversions. The regulations permit the taxpayer to recharacterize (undo) the taxable Roth IRA conversion at any time during the year of conversion or by the filing date of the individual's tax return, including extensions. As a result, a recharacterization can be made as late as Oct. 15 of the year following the year of conversion.

A variety of reasons could cause an individual to change their mind about a prior conversion event, including:

- Tax results of the conversion were misjudged
- Impact of changes to future tax rates could affect the decision
- Subsequent change in investment performance of the converted amount

Reconvert

In turn, an individual may subsequently choose to reconvert their recharacterization. However, a reconversion may only take place at the later of the following two dates:

- The tax year following the original conversion
- 30 days after the recharacterization.

These provisions are in place to give an individual some flexibility and should be referred to your tax advisor and investment professional to assure you manage your circumstances to the best outcome. For more information contact your local Eide Bailly tax advisor. ■

Do You Know Who You Are Hiring?

Kari Yonke, Forensic Accounting Manager

In today's uncertain economy, you want to make sure your organization has honest and trustworthy employees. The best way to do this is to make sure you are doing your due diligence by regularly conducting background check before hiring a new employee.

More and more job-seekers are including misleading information on their resumes, especially during a recession when jobs are hard to get. A background check can help confirm information like job titles, dates of employment, credentials and education.

Background checks give hiring managers the proper information, and the confidence, to make the right hires; it is important to verify an applicant's resume, as misleading information could make him unqualified for a particular position.

We recommend companies implement a formal policy to ensure background checks are used consistently in the hiring process. This can help protect your company from unnecessary risk. For more information visit our website at www.eidebailly.com ■

Focus on the Forest – Not the Trees

As the market goes up and down, it's easy to become too focused on day-to-day returns. Instead, keep your eyes on your long-term investing goals and your overall portfolio. Although only you can decide how much investment risk you can handle, if you still have years to invest, don't overestimate the effect of short-term price fluctuations on your portfolio.

When the market goes down, and investment losses pile up, you may be tempted to pull out of the stock market altogether and look for less volatile investments. The small returns that typically accompany low-risk investments may seem attractive when more risky investment are posting negative returns. But before you leap into a different investment strategy, make sure you're doing it for the right reasons. How you choose to invest your money should be consistent with your goals and time horizon.

To read the full article, go to <http://www.eidebailly.com/services/financial-services/handling-market-volatility>. ■

Content provided by Forefield, Inc. Neither Forefield Inc. nor Forefield Advisor™ provides legal, taxation or investment advice. All the content provided by Forefield is protected by copyright. Forefield claims no liability for any modification to its content and/or information provided by other sources. © 2011 Forefield Inc. All Rights Reserved.

Financial Advisor is a Registered Representative of and offers securities through Securities America, Inc. Member FINRA and SIPC. Investment Advisory Services offered through Eide Bailly Advisors, LLC, a Registered Investment Advisor. Eide Bailly Financial Services, LLC is the holding company for Eide Bailly Advisors, LLC. Eide Bailly Financial Services and its subsidiaries are not affiliated with Securities America companies.

2011-2012 Business Tax Planning

Summary of Tax Depreciation Incentives

Time is growing short to take advantage of two special depreciation expense deductions. The Bonus Depreciation Incentive is available for new business assets. The Section 179 Depreciation Incentive is available for new and used business assets. The following table explains the requirements a business asset must satisfy to be eligible for the depreciation incentives in 2011 and/or 2012.

Requirements	Bonus Depreciation	Section 179 Depreciation
The asset must have been purchased in 2011 or 2012.	Businesses can write off up to 100% of the cost of 2011 purchases or 50% of 2012 purchases. <ul style="list-style-type: none"> Only new assets qualify and must have a prescribed tax life of less than 20 years Certain aircraft property, lengthy-production period. Assets or certain reconditioned property also may qualify 	Movable equipment or special purpose assets can be 100% expensed in the year acquired. <ul style="list-style-type: none"> either new or used equipment are eligible or special accelerated depreciation expense the deduction is deferred if the business reports and overall net loss for the tax year of the asset purchase.
The asset must meet the depreciation incentive's required service dates.	The 100% write-off applies to assets purchased between Sept. 8, 2010, and Dec. 31, 2011. Purchases made during the year 2012 are eligible for a 50% write-off.	The provision applies to purchases made between Dec. 31, 2010, and Dec. 31, 2012. <ul style="list-style-type: none"> as much as \$500,000 in 2011, then declines to a \$125,000 cap in 2012
The asset amount must fall under the annual dollar ceiling for maximum tax benefit.	No annual dollar ceiling	Not available if more than \$2 million in 2011, or \$500,000 in 2012 of tangible property purchased during the tax year.
The asset must satisfy the related party limitations.	Related party purchases may qualify for bonus depreciation in some situations. Call your Eide Bailly tax advisor for clarification.	Related party purchases do not qualify for Section 179.
Vehicles must comply with special restrictions: <ul style="list-style-type: none"> Pick-up or truck with six-foot truck beds Heavy SUVs more than 6,000 Gross Vehicle Weight (GVW) <ul style="list-style-type: none"> must be greater than 50% business use 	New pickups or trucks with six-foot truck beds or heavy SUVs are eligible for a 100 percent write-off in 2011. <ul style="list-style-type: none"> The maximum 2012 vehicle bonus depreciation for greater than 6,000 GVW vehicles is only up to 50 percent of the purchase price. 	New or used vehicles are eligible if more than 6,000 GVW and greater than 50% business use, up to \$25,000 annual ceiling in 2011 and 2012
Lighter weight vehicles carry special rules: <ul style="list-style-type: none"> Light pick-up or SUV under, 6,000 GVW 	A greater than 50% business useage percent of cost multiplied by the \$11,260 limit in 2011, 2012.	A greater than 50% business useage percent of cost multiplied by the \$11,260 limit in 2011, 2012.
The asset is a qualified leasehold improvement paid by the tenant or landlord in 2011.	Interior, non-structural improvements to a greater than three-year old, nonresidential, commercial structure qualify for 100 percent bonus depreciation in 2011. <ul style="list-style-type: none"> not applicable if leased to or from a related party 	Section 179 expensing is available for Qualified Leasehold Improvements to a greater than three-year old commercial structure in 2011. <ul style="list-style-type: none"> the 2011 dollar ceiling is \$250,000 in 2012, the dollar ceiling declines to zero
The asset is qualified <i>retail</i> or qualified <i>restaurant</i> improvements (nonstructural only) paid by the tenant or landlord in 2011.	2011 Bonus Depreciation is not permitted for these two categories of building improvements. If placed in service before Dec. 31, 2011, a 15-year depreciable life is permitted on the remaining cost of the asset.	Section 179 expensing is available for Qualified Retail or Qualified Restaurant leasehold improvements in 2011 (the dollar ceiling is \$250,000). <ul style="list-style-type: none"> If placed in service before Dec. 31, 2011, a 15-year depreciable life is permitted on the remaining cost of the asset.
Limitations affecting the non-corporate lessor are satisfied by the asset's owner	The property must be used in a business.	Section 179 may not be allowed to landlords/owners who arrange a net lease of tangible property with their tenant. <ul style="list-style-type: none"> Non-corporate landlord/owners must satisfy the 15 percent expense ratio and lease the asset for less than 50% of its life to qualify for Section 179 benefits.

State Tax Depreciation Incentives are often different than the Federal Income Tax provisions described in the above chart. Numerous choices are offered to the expanding business. Contact your Eide Bailly tax advisor to plan for the greatest advantage in 2011, 2012 and beyond.



CONTACT

Joy Culver
Partner
406.896.2428
jculver@eidebailly.com



CONTACT

Kathy Pangburn
Senior Tax Associate
406.896.2417
kpangburn@eidebailly.com

Spear Phishing:

A New Danger for Small Businesses

You've got a lot on your mind if you run a small business. Payroll to make, people to supervise and manage, sales to make and books that need to be balanced. Does the thought that you and your business could become the target of international thieves ever cross your mind?

It should. Small businesses have become the latest target for international thieves the last few years. They approach your business in its weakest spot: as a potential sale. They use information from that approach to drain your bank account quicker than you can hang up the phone. It's called spear phishing and it's not about fish. It's about targeting (that's the spear) your business to get information (the object of the phishing) that can be used to drain your bank account.

Here's how it works:

The scam starts with a telephone call, an e-mail or a fax. The pitch is something like this: "We are in need of a supplier for (insert your product here). We need (large amount, larger than your typical sale to one customer) units of this product. We expect to have an ongoing purchasing arrangement if you can supply our needs." They may go on with background material about how their business has picked up and you may learn more about them than you really want to know.

There may be several contacts, or just a few, and they may even sign a contract. The part you need to watch for is when they say something like, "We will pay you via ACH transfer (direct deposit or electronic funds transfer) since that is the cheapest way for us to pay you. You'll get your funds that much quicker. Please fill out this form from our bank with your banking information and fax it or scan it and e-mail it to our bank." The form will request your bank's information, including the routing number and your account number. Once the con artists have this, the honeymoon is over. The next step is for them to steal your money.

How?

The con artists will use the information to contact your bank by e-mail, telephone or fax, and request a wire transfer out of your account. They will pretend to be you. Since they possess information about your account, their associates will have targeted other phishing attempts to gather your identifying information, such as tax identification number, e-mail addresses and contact phones. The con artists may have even copied your letterhead and logo if they're submitting the request by fax. The

money will be transferred out of the U.S. banking system to a foreign country.

Now, you have officially been had. The bank will blame you for not protecting your data. You will blame the bank for wiring your money to a country where you probably have never done business. Law enforcement won't be much help because U.S. law enforcement has no authority in a foreign country, and the local law enforcement in the country where the money was sent may be part of the scheme or taking payments from the crooks. Your lawyer may not be able to help because the case law is not settled on this, so it can go either way.

What should you have done?

Prevention is the only sure way to not lose money from a fraud scheme. Prevention is money and time you invest in your business up front so you don't have to spend more money and time later chasing lost money.

What prevents this from occurring? Policies, Procedures, and Training

- Policies must be in writing and clearly spell out what information is allowed to be disclosed to people or businesses outside of your company and under what circumstances.
- Procedures also must be in writing and should try to identify as many potential scenarios asking for sensitive information as possible and identify the appropriate way of handling those requests.
- Train your staff, especially management, in the policies and procedures. New staff must be trained in information security as soon as possible. Emphasize that information is money and disclosing too much information can kill your company and put them out of a job.

To read the full article, go to <http://www.eidebailly.com/services/forensic-valuation/spear-phishing-a-new-danger-for-small-businesses>. ■



CONTACT

Danny Reynolds, MPA, CFE, CFCE, CAMS
Forensic Accounting Manager
605.977.2727
dreynolds@eidebailly.com

Got Mobile?

Learn How to Properly Protect Your Business and Personal Data

Security is everyone's business. If you think security is all network related, then think again. While companies (even information technology (IT) managers) often throw more money at IT investments when security breaches arise, many security breaches are actually people-related issues that can be easily managed, if not prevented.

There's no denying that the hackers' playing field has broadened globally through the recent explosion of mobile devices, such as laptops, smart phones and tablets. Data has never been so easily accessible, nor widely available as it is today. As these devices become more powerful, they can hold much more information than ever before. Add to that our tendency to carry both business and personal information on the same device and your risk becomes even greater. However, you don't have to compromise convenience of technology for safety.

You can save your company, your clients and your family time and money by becoming aware of the threats, vulnerabilities and counter measures you can take to mitigate the risk of being attacked and by securing your assets and sensitive data.

Examples of sensitive data include:

- Employee's personal data
- Operational Plans
- Trade secrets
- Business Intelligence
- Marketing Plans
- Product Information
- Business Plans

What can you do to prevent and/or detect hacking?

- 1 **Watch your apps** – while some companies, such as Apple, have strict standards for the types of applications made available online for iPods/iPads, most tablets use Android technology, which is wide open to developers and millions of free applications that may be infected.
 - Do some due diligence and resist the temptation to download applications from unknown or un-reputable companies.
 - Read reviews from other users who have downloaded applications.
 - Avoid downloading applications from companies asking for private data or notifying you that a third-party application is requesting private information.
 - Even if an application is made available on a reputable site, the application itself may not be safe.
- 2 **Safeguard servers in a secure location** – physically lock the area where your assets are located and limit access to those who can access it.

Develop and enforce technology policies – There are many resources that provide guidance on the treatments of company information and assets. Make these policies a priority!
- 3 **Use security monitoring services** – an ounce of prevention is your safest bet is to hire a third-party to act as your burglar alarm. People are your greatest asset and they are much smarter and intuitive than systems or software at detecting potential threats.
- 4 **Keep a close eye on your assets** – when you travel, be sure to secure your laptop or other mobile device. If your equipment is misplaced, lost or stolen, you may be disclosing information about your company and its customer base. Under federal law, your company would have to notify potentially millions of people whose data was compromised and this is an easy and costly mistake.
- 5 **Use a VPN** – if you have access to a VPN (virtual private network), use it. A VPN provides secure access to the network and allows you to get online behind a secure layer that helps protect your information. You should also avoid unencrypted public wireless networks, such as Wi-Fi networks where no authentication or password is needed to log in. Not only can you log in, but so can the bad guys.
- 6 **Even encrypted networks**, (those that require an ID or password for access), such as WEP (wired equivalent privacy) and WPA (Wi-Fi protected access) have risks, and it's possible for hackers to gain access. Be cautious about how you use these networks. In addition, turn off Wi-Fi when you're not using it. This will prevent you from automatically connecting to networks (and will extend your device's battery life).
- 7 **Employ strong passwords or devices** – Try using a combination of letters, numbers and/or special characters of eight or more.

Hacking—continued on page 8

Medicare: An Awareness Discussion



Medicare is a program designed by the federal government to provide health care insurance to people age 65 or older.

According to the PEW Research Center, about 10,000 baby boomers will turn 65 every day for the next 19 years. Similarly, many of them will begin enrolling in Medicare. We hear a lot about Medicare. Payroll taxes are taken from wages and self-employed earnings are dedicated to the Medicare program. However, most baby boomers don't really understand Medicare. What is Medicare? How is it different from Medicaid?

Medicare is a program designed by the federal government to provide health care insurance to people age 65 or older. People younger than 65 can also qualify for Medicare if they have disabilities, permanent kidney failure or Lou Gehrig's disease. The primary purpose of Medicare is to assist the payment of health care costs after reaching retirement age, which for Medicare, remains at age 65.

Medicaid is not the same program as Medicare. Both deal with health care costs, but Medicaid is not sponsored by the federal government. It is a state-run program designed to provide hospital and medical coverage to individuals with low income. Because Medicaid programs are provided and financed by the states, each program may have different rules for eligibility and coverage.

Medicare is divided into four parts. An electing participant can select the coverage (called parts) they want. The four parts of Medicare include:

- Part A - Hospital Insurance
- Part B - Medical Insurance
- Part C - Medicare Advantage
- Part D - Prescription Drug Coverage

While Medicaid is paid for by the states, Medicare is paid for by the current and future participants (sometimes referred to as beneficiaries). Current beneficiaries pay a monthly premium typically deducted from Social Security checks. Future beneficiaries finance the program through withholdings made on wages and self-employment income.

The current beneficiary's premium is based on the Medicare parts selected and the taxable income level. Higher income beneficiaries pay a higher monthly premium. The current Medicare tax rate for future beneficiaries applied to all wages and self-employment earnings is 2.9 percent. However, only a self-employed person pays the full 2.9 percent. An employee is responsible for half, or 1.45 percent, of the total, with an employer picking up the other 1.45 percent.

A potential Medicare beneficiary should sign up for Medicare three months before or after the month they have their 65 birthday, even if they do not plan to retire at age 65. Signing up for Medicare at 65 will eliminate a 10 percent premium increase for each 12-month period a person was eligible for, but did not enroll.

There is a special enrollment period for a person 65 or older covered under a group health plan from personal, current employment or from a spouse's current employment. The special enrollment period allows for a delay in enrollment, while currently covered under an employment group health plan, or as late as eight months following the last month of coverage or employment.

For more information about Medicare, go to www.medicare.gov or call 1-800-MEDICARE (1-800-633-4227). Additional information also is available at www.socialsecurity.gov. ■



CONTACT

Larry Evans, CPA
Partner
405.858.5500
levans@eideabilly.com

A Blue Ribbon Panel Update

Where Is Private Company Accounting Going?

The Issues

In 1973, the Financial Accounting Foundation created the Financial Accounting Standards Board (FASB) to set accounting standards for public and private entities. However, in the last 30 years, many practitioners believe the standard setting process has changed in several significant ways.

- First, FASB has increasingly added significant complexity to the accounting rules, thereby making compliance more difficult.
- Second, pushed by Congress after the failure of Enron in 2002, the Securities and Exchange Commission (SEC) has gained increasing influence over the rules-making process of the FASB, and has geared accounting toward large public rather than smaller private companies.
- Lastly, the SEC has pushed for convergence of U.S. accounting standards with those of Europe. Relevance to private companies is the issue.

Response

In 2009, several stakeholders came together to sponsor the Blue Ribbon Panel on Standard Setting for Private Companies to study the issues. Comprised of academicians and representatives from public accounting firms and private companies, the panel began to research the problems, and possible solutions.

The panel reaffirmed the above issues and concluded the disproportionately large private company group:

- Was generally underserved by the current standard setters,
- Received inadequate focus on decision-useful needs of private company financial statement users and

- Was burdened with standards where compliance costs appear to often exceed the benefits.

In January 2011, the Panel published its formal “Report to the Board of Trustees of the Financial Accounting Foundation.” The report proposed two major changes to the current system, including:

- A new private company standards board, apart from FASB, to make accounting rules solely for private companies; and
- New accounting standards tailored to private companies.

The new board would be representative of the private company sector and sensitive to private company needs.

The Blue Ribbon Panel has begun to address the problems with current private company accounting. The Financial Accounting Foundation recently announced the establishment of a working group as the next phase of its review of the adequacy and effectiveness of the Financial Accounting Standards Board’s efforts in setting standards for the private company sector. The Foundation hopes to have further and final recommendations this fall. ■



CONTACT

Jim Boak, CPA
Partner
303.539.5904
jboak@eidebailly.com

Tax Reform—from page 1

current tax rates not set to expire until after Dec. 31, 2012, aside from some credits and deductions already set to expire in 2011, tax reform changes for 2012 will be hard to pass in an election year.

Is 2013 the effective year for general tax reform?

It would seem to depend on how realistic Congress becomes in trimming the national debt and who gets the credit for the reduction.

Republicans favor spending cuts, while democrats want increased tax revenue, particularly from those making more than \$250,000. However, it will probably take both spending cuts and new tax revenue, which if properly communicated and consistently applied, most taxpayers will probably support.

It is not knowing the tax structure that will be in place over a long period of time and the increasing administrative costs that damages any business expansion and tax planning efforts.

Whatever Congress decides, time will help solve the economic slide, with or without general tax reform. With no profit growth potential, taxes become much easier to plan. ■



CONTACT

Larry Evans, CPA
Partner
405.858.5500
levans@eidebailly.com



4310 17th Ave S
PO Box 2545
Fargo ND 58108-2545

RETURN SERVICE REQUESTED

This publication is produced and published by Eide Bailly and distributed with the understanding that the information contained does not constitute legal, accounting or other professional advice. It is not intended to be responsive to any individual situation or concerns as the contents of the publication are intended for general informational purposes only. Readers are urged not to act upon the information contained in this publication without first consulting competent legal, accounting or other professional advice regarding implications of a particular factual situation. Questions and information for publication can be submitted to your Eide Bailly representative.

To request reprints of this publication, send a written request to ReprintRequest@eidebailly.com. © 2011 Eide Bailly LLP.

To view this and previous issues of **POSSIBILITIES**, visit www.eidebailly.com/publications

Managing Editor: Liz Stabenow
Assistant Editor: Sadie Rudolph
Send comments to: possibilities@eidebailly.com

**An Independent Member Firm
of HLB International**



www.eidebailly.com

Hacking—from page 5

Create acronyms for things you'll remember, such as your favorite foods, songs and other items only you would know. Change your passwords frequently. Also, don't write your passwords down. Instead, use a device, such as a password keeper, to store important passwords.

8 *Educate your staff* – hold regular meetings to make employees aware of your policies, threats and consequences of enabling a breach. Most employees are not even aware of the potential impact this may have on a business and to the bottom line. Security can be as easy as not clicking on a link, or opening an attachment in an e-mail.

9 *Make sure software is up-to-date* – nearly every release of software patches a number of security vulnerabilities that are out there. Check regularly to see if an update is available. If there's a new one, download it, unless there are negative reviews from early adopters.

10 *Look beyond the obvious* – consider investing in new tactics, such as social engineering services (also referred to as people hacking), to test your staff for potential security breaches.

Treat the Situation like a Crime Scene

What do you do if you've been or suspect you've been hacked?

- Immediately secure the area and disconnect your system to prevent further hacking. This will enable you to isolate the issue as well.
- Don't disturb the "crime scene." Leave everything as is until an investigation can be ordered.
- Dig up and document details about the breach, such as time, date, possible cause, etc. If your case goes to court, it's important that you have as much evidence as possible.
- Interview employees, such as systems administrators, who may be involved in causing or detecting the breach.
- Call in a forensics team! Contact a third-party vendor immediately to investigate the cause and provide prescriptive guidance on how to fix it. They will also suggest ways to prevent it from happening again. ■



CONTACT

Jeremiah Talamantes
CEH, CISSP
Senior Security Consultant
952.918.3527
jtalamantes@eidebailly.com