Kakimoto & Nagashima LLP
Certified Public Accountants
Consultants

NEWSLETTER

Volume 13, Issue 1 January 2015

Inside this issue:

Any Questions?

We are committed to providing our clients with quality and excellent services. If you have any questions or comments, please let us know by either e-mail or phone. Our company profile is available on the internet at:

http://www.knllp.com

Tel: (310) 320-2700
Fax: (310) 320-4630
E-mail: sboffice@knllp.com

Summary of Articles

New Going Concern Standard Issued (ASU 2014-15)

In August 2014, the FASB issued a new going concern standard, ASU 2014-15, "Disclosure of Uncertainties about an Entity's Ability to Continue as a Going Concern". This standard defines and provides guidance on management's responsibility to evaluate whether there is substantial doubt about an entity's ability to continue as a going concern. Highlighted in this article are the new ASU's key provisions; companies will need to determine how much of an impact this new accounting standard will have on its financial reporting and disclosure.

One-Year Tax Extenders Bill Now Law

With the passing of the Tax Increase Prevention Act of 2014 into law, many temporary tax deductions, credits, and incentives (also known as "tax extenders") that were to originally expire on December 31, 2013 have been retroactively extended for one year. This article lists a few notable tax extenders that are available for taxpayers to utilize on 2014 tax returns.

Beware of IRS Tax Scams

Have you been contacted by the IRS? Have you been asked to provide personal financial information? Whether or not you've been contacted, you should be aware that there has been an increase in identity theft scams in which the scammers claim to be from the IRS. To learn more about these scams, please read the article in this edition of our newsletter.

How Secure is Your Password?

In light of the recent Sony hacks, it has become apparent that cyber security should be ever present and fiercely maintained within all corporate environments. But the decision to maintain high level security should not only fall on the heads of network administrators. The average user can play a hand in keeping your network secure. The most basic level of protection that users can incorporate is to use complex passwords for login credentials. Read on for a simple guideline you can follow to create one for yourself.

Kakimoto & Nagashima's future newsletters will only be published on-line for your convenience. Please make sure we have your current e-mail address by registering with us at:

http://www.knllp.com/newsletter/registration.php

We look forward to providing you with up-to-date accounting and tax information.

ASU 2014-15 - Going Concern Reporting Responsibilities - Now Part of U.S. GAAP

In August 2014, the Financial Accounting Standards Board ("FASB") issued ASU 2014-15, "Disclosure of Uncertainties about an Entity's Ability to Continue as a Going Concern" ("ASU 2014-15"), to provide U.S. GAAP guidance regarding management's responsibility to evaluate an entity's ability to continue as a going concern and applicable disclosure requirements. The new standard incorporates and expands upon certain principles found in U.S. auditing standards.

ASU 2014-15 Key Provisions

Management Assessment

For each reporting period (including interim periods), an entity's management will be required to evaluate whether there is substantial doubt about an entity's ability to continue as a going concern and provide the required disclosures when substantial doubt exists. The new standard defines substantial doubt as follows:

> "Substantial doubt about an entity's ability to continue as a going concern exists when conditions and events, considered in the aggregate, indicate that it is probable that the entity will be unable to meet its obligations as they become due within one year after the date that the financial statements are issued….."

The term "probable" is used consistently with its current use in ASC 450, "Contingencies".

Management's evaluation should be based on relevant conditions and events that are known and reasonably knowable at the date the financial statements are issued (or available to be issued, when applicable). Quantitative and qualitative information should be used by management in its evaluation. Substantial doubt exists if it is probable that the entity will be unable to meet its obligations within one year after the issuance date.

When management identifies conditions or events that raise substantial doubt about an entity's ability to continue as a going concern, management's plans to mitigate these conditions or events should be evaluated to determine whether substantial doubt is alleviated. The mitigating effect of management's plans should be considered only to the extent that:

- it is probable that the plans will be effectively implemented and, if so,
- it is probable that the plans will mitigate the conditions or events that raise substantial doubt about the entity's ability to continue as a going concern.

If there are no conditions or events that give rise to substantial doubt, no disclosures will be required specific to going concern uncertainties, however, areas including risks and contingencies may require certain disclosure.

Disclosures

Disclosures will be required if substantial doubt is raised whether or not the substantial doubt is alleviated by management's plans.

If substantial doubt regarding an entity's ability to continue as a going concern is alleviated after consideration of management's plans, the following information should be disclosed:

- Principal conditions or events that raised substantial doubt about the entity's ability to continue as a going concern (before consideration of management's plans).
- Management's evaluation of the significance of those conditions or events in relation to the entity's ability to meet its obligations.
- Management's plans that alleviated substantial doubt about the entity's ability to continue as a going concern.

If substantial doubt is not alleviated after the consideration of management's plans, the entity should disclose the following:

- A statement indicating that there is substantial doubt about the entity's ability to continue as a going concern within one year after the date the financial statements are issued.
- Principal conditions or events that raised substantial doubt about the entity's ability to continue as a going concern.
- Management's evaluation of the significance of those conditions or events in relation to the entity's ability to meet its obligations.
- Management's plans that are intended to mitigate those conditions or events that raise substantial doubt about the entity's ability to continue as a going concern.

Effective Date

For all entities, ASU 2014-15 is effective for the annual period ending after December 15, 2016, and for annual periods and interim periods thereafter. Earlier application is permitted.

Kakimoto & Nagashima LLP is dedicated to providing our clients with quality service and experience. We are also committed to professional standards and assisting our clients to understand the new and significant changes in those standards. If you should have any questions or comments, please do not hesitate to contact us. ♦

One-Year Tax Extenders Bill Now Law

On December 19, 2014, President Obama signed into law the Tax Increase Prevention Act of 2014. Among other provisions, this new law retroactively extends for one year numerous temporary tax deductions, credits, and incentives (also known as "tax extenders") that were to originally expire on December 31, 2013. With passage of this bill, taxpayers will be able to utilize these tax extenders on their 2014 tax returns.

The following is a list of a few notable tax extenders that have been retroactively extended through December 31, 2014:

For Individuals

- Deduction for state and local general sales taxes in lieu of state and local income taxes;
- Above-the-line deduction for qualified tuition and fees for post-secondary education;
- Treatment of mortgage insurance premiums as deductible interest that is qualified residence interest; and
- Exclusion of income from the cancellation of mortgage debt on a qualified principal residence.

For Corporations

- Increased expensing under Code Section 179 - Allows immediate deduction, rather than gradual depreciation, of the cost of qualified assets, with limits of $500,000 for deduction and $2 million for overall investment;
- Bonus depreciation – additional first-year depreciation deduction of 50 percent of the basis of qualified property;
- Election to accelerate Alternative Minimum Tax credits in lieu of bonus depreciation;
- 15-year straight-line depreciation for qualified leasehold improvements, qualified restaurant property, and qualified retail improvements; and
- Research tax credit for increases in qualified research expenditures.

Please note that this article does not cover all tax extenders that have been retroactively extended by the Tax Increase Prevention Act of 2014. If you have questions pertaining to this issue, please contact the office of Kakimoto & Nagashima LLP at (310) 320-2700.♦

Beware of IRS Tax Scams

As identity theft has been a growing problem in recent years, so has the prevalence of scams using the IRS name. Scammers have been employing schemes through email, fax, or telephone that fraudulently use the IRS name, logo or website to gain access to taxpayers' personal and financial information in order to steal their identities and assets. It is extremely important, therefore, that taxpayers be aware of such scams in order to protect themselves from identity theft and financial loss.

Based on a February 2014 Department of Justice news release, from 2008 through May 2012, the IRS identified more than 550,000 taxpayers who have had their identities stolen for the purpose of claiming false refunds in their names.

Currently, one of the most common schemes is a widespread phone scam in which taxpayers (often recent immigrants) receive unsolicited phone calls from individuals demanding payment while fraudulently claiming to be from the IRS. In these cases, potential victims may be told that they are entitled to a large refund, or that they owe money that must be paid immediately to the IRS; callers then attempt to trick the potential victims into providing personal and financial information. Callers frequently use an insulting or hostile tone and threaten potential victims with deportation, arrest, revocation of their driver's license, or having their utilities shut off if immediate payment is not made. If the call is not answered initially, scammers will often leave an urgent callback request.

The following is a list of additional characteristics of this scam:

- Scammers use fake names and IRS badge numbers, and they generally use common names and surnames to identify themselves.
- Scammers may be able to recite the last four digits of the taxpayer's Social Security number.
- Scammers alter the caller ID to create the appearance that it is indeed the IRS that is calling.
- Scammers will sometimes also send fake IRS emails to support their phone calls.
- Recipients of the phone calls hear background noise of other calls being conducted to mimic a call site.
- After being threatened with arrest or driver's license revocation, potential victims may soon receive additional calls from scammers claiming to be from the local police or Department of Motor Vehicles, with their caller ID supporting their claim.
- Potential victims may be told that they must pay the money owed promptly by pre-loaded debit card or wire transfer.

To avoid falling victim to these telephone scams, individuals should note that scammers often do the following things that the IRS will never do:

- Call individuals about taxes owed without first sending them an official notice via U.S. mail.
- Demand that individuals pay taxes without allowing them the opportunity to question or appeal the amount claimed to be owed.
- Require individuals to use a specific payment method for taxes, such as a prepaid debit card.
- Ask for debit or credit card numbers over the phone.
- Threaten to bring in local police or other law-enforcement groups to arrest individuals for not paying.

By taking note of the above points, potential victims can identify an IRS call as fake fairly easily.

As mentioned previously, scams can also be initiated through email; such scams are referred to as "phishing". One of the newest phishing scams is one in which taxpayers receive emails that appear to be from the IRS and include a link to a fake website intended to replicate the official IRS website. The intention of the fake website is to lure taxpayers into providing personal and financial information. The emails contain the instruction, "you are to update your IRS e-file immediately", and they refer to IRSgov, not IRS.gov.

Another phishing scam uses emails or text messages to lure taxpayers to a malicious website. These messages inform recipients that a federal tax transaction recently initiated from their checking account was "rejected by the Electronic Federal Tax Payment System". The scammer's email address is disguised as a legitimate IRS account (irs@service.govdelivery.com).

It is important to note that the IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and any social media. The IRS also does not ask for PINs, passwords, or similar confidential access information for credit card, bank, or other financial accounts.

A scam of which non-residents of the U.S. should be aware is one in which they receive a fake IRS letter and Form W-8BEN (Certificate of Foreign Status of Beneficial Owner for United States Tax Withholding) asking them to provide personal information such as account numbers, mother's maiden name, and passport number. The legitimate IRS Form W-8BEN, which is used by financial institutions to establish appropriate tax withholding for foreign individuals, does not ask for any of this information.

The IRS recommends certain procedures to take when encountering a scam. If you receive a phone call from someone claiming to be from the IRS, you should do the following:

- If you know you owe taxes or think you might owe taxes, call the IRS at 1-800-829-1040. IRS employees at that number can help you with a payment issue, if one indeed exists.
- If you do not owe taxes or have no reason to think that you owe any taxes, call and report the incident to the Treasury Inspector General for Tax Administration (TIGTA) at 1-800-366-4484 or at www.tigta.gov.
- You can file a complaint using the Federal Trade Commission (FTC) Complaint Assistant at www.ftccomplaintassistant.gov.

Regarding phishing scams, recipients of an email should take the following steps:

- Do not open any attachments.
- Do not click on any links contained in the message.
- Forward the email to phishing@irs.gov.

Please note that this article does not cover all information regarding IRS scams, as the types of schemes used by identity thieves extend beyond those addressed above. If you have questions pertaining to this issue, please contact the office of Kakimoto & Nagashima LLP at (310) 320-2700.♦

How Secure is Your Password?

Many in the technology industry might just classify the year of 2014 as the year of the security breach. From the high profile story of the infamous Sony Hack to the Heartbleed OpenSSL zero day vulnerability. In addition there have also been numerous reports of Instagram, Pinterest, Yahoo, and even Google accounts being compromised. We all live in a connected world. Our lives are out there for everyone to see. On display forever on the internet. We need to be protected.

One of the easiest things that we can do as individuals, to protect ourselves is using complex passwords for all of our online accounts. From bank websites to Facebook, a difficult to guess password is the most basic form of security we can all implement. Passwords are your last line of defense against prying eyes.

Everyone Has Enemies

An important thing to keep in mind is that we all have someone that is out to get us. A former co-worker whom you were promoted in front of. A heartbroken ex-girlfriend or boyfriend. An intrusive spouse, nosy parents or just someone who doesn't really like you. Regardless of whom it is, there may be someone trying to break into your accounts to take a peek into your personal life.

If your passwords use numbers or passphrases from your personal life, the easier it is for someone to hack you. If these people know you well, they might be able to guess your e-mail password and use password recovery options to access your other accounts.

The other end of the spectrum would be hackers. Their method of attack is using brute force methods to identify your password. These attacks work by systematically checking all possible passphrases until the correct one is found. If the hacker already has an idea of the guidelines used to create the password, this process becomes easier to execute.

It has been reported that the recent Sony Hacks were not all that sophisticated and that compromised passwords are a likely vector of infiltration in the hack. The insufficient corporation-wide password standard being used by Sony led to the simplicity of the attack. Also reported was that the CEO of Sony Entertainment, Michael Lynton, was apparently using an embarrassingly simple password.

Microsoft's Guide on How to Create a Secure Password

To help you create strong passwords, follow the same network security guidelines required of all Microsoft employees:

- Strong passwords are phrases (or sentences) at least eight characters long—longer is better—that include at least three of the following: uppercase and lowercase letters, numerals, punctuation marks, and symbols.
- Give passwords the thought they deserve, and make them memorable. One way is to base them on the title of a favorite song or book, or a familiar slogan or other phrase. (Don't use the examples below!)
  - *Example phrases: I love my new Xbox One
  - *Example passwords: Ilove!mynewxbox1
- Don't share passwords with others or store them on the device they're designed to protect.

Once you've come up with your password, you can test its strength at this website - https://www.microsoft.com/security/pc-security/password-checker.aspx

Avoid Common Password Pitfalls

Cybercriminals use sophisticated tools to rapidly crack passwords, but you can help foil their attempts.

DO NOT USE:

Personal identity information that could be guessed or easily discovered, like pet names, nicknames, birth date, address, or driver's license number.

Dictionary words in any language (including the word password—the most common password in the English language!).

Words spelled backwards, abbreviations, and common misspellings (accommodate, remember).

Common letter-to-symbol conversions, such as changing "o" to "0" or "i" to "1" or "!".

Sequences or repeated characters. Examples: 12345678, 222222, abcdefg, or adjacent letters on your keyboard (such as qwerty).

Enable Two-Step Verification

Any time a service like Facebook or Gmail offers "two-step verification," use it. When enabled, signing in will require you to also enter in a code that's sent as a text message to your phone. Meaning, a hacker who isn't in possession of your phone won't be able to sign in, even if they know your password. You only have to do this once for "recognized" computers and devices.

Having a password policy in your corporate network infrastructure is a vital piece in keeping your network secure. Following the guidelines here can help you improve your policies currently in place. Should you need help in examining your policy, give the office of Kakimoto & Nagashima LLP a call and we will gladly be of service.♦

Basic Rules for Password Privacy

- Don't write it down.
- Devise a password-creating system that's all yours.
- Don't send your password via e-mail or give it out over the phone.
- Disable AutoComplete for user names and passwords.
- Change your password often.
- Clear the cache after using a public PC.
- Use a password-management utility.

Questions or comments about this issue or inquiries about our newsletter by e-mail subscription service can be sent to:

newsletter@knllp.com