

madan

CHARTERED ACCOUNTANT

5113 Heritage Hills Blvd.
Mississauga, ON L5R 2C6
Telephone: 905.268.0150
Facsimile: 905.507.9193

VOLUME 24, ISSUE 1
February 2010

INDEX

TAXATION

Taxation Tools

MONEYSAVER

Check Your Cheques

TECHNOLOGY

Learning from a Worm

MANAGEMENT

The Budding Entrepreneur

TAXATION

Taxation Tools

Tradespersons can enjoy a tax deduction for new tools while anyone wanting to build a nest egg outside an RRSP needs to know about the Tax Free Savings Account.

For the Tradesperson...Tools of the Trade

Tradespersons earning income from the use of their tools may be entitled to deduct the cost of eligible tools plus the GST, PST, or HST included in the invoiced price. Just what is deductible depends on the trade; however, tools will generally be considered deductible if:

- the tool is new and for use in your trade; and
- your employer provided the appropriate signed form **T2200, Declaration of Conditions of Employment**, indicating that supplying the tool was a condition of employment and necessary for your job. Electronic equipment for measuring, locating or calculating are included but cell phones and other communications devices are not.

It is recommended that tradespersons save a list of all new tools and attach the invoices to the listing. In the event the Canada Revenue Agency wishes to confirm the deduction, the data will be readily available.



The maximum deduction in 2009 is the lesser of \$500 or the amount paid for the tools minus \$1,044. Thus, if the tradesperson spends \$3,000 on tools, the maximum deductible allowable would be the lesser of \$500 or the amount resulting from application of the formula, i.e. $\$3,000 - \$1,044 = \$1,956$. In this case the maximum deduction would be only \$500. To claim your tool expense, enter the claim on **Form T777**.

If the tradesperson is employed and reported employment income for 2009, like all other employees, an additional \$1,044 may be claimed as a credit on line 363 of schedule 1. This credit, known as the Canada Employment Amount, need not be justified. It recognizes work-related expenses including such items

as home computers, uniforms, and supplies. Self-employed persons are not eligible to claim this amount.

For the Nest Egg...TFSA's

Tax Free Savings Accounts are a great idea for those who expect to earn investment income on excess funds. It may be a better alternative than an RRSP in certain cases.

TFSA's are a great alternative to those who have maximized their RRSP contributions and wish to earn income without the threat of additional income tax on investment returns. Whereas an RRSP investment permits an immediate tax savings in the year of investment and is taxed only when withdrawn, the TFSA operates in reverse; the funds you place in a TFSA are after-tax dollars but any growth through capital gains, dividends or interest can be removed tax free. For individuals whose RRSP withdrawals, combined with other sources of income, will place them in a higher individual tax bracket in later years, a TFSA may be a viable alternative to ensure additional future income without the accompanying higher tax cost.

As with all government initiatives rules and regulations are the norm. Here are some pointers about TFSA's:

1. They can be set up through a bank, credit union or other financial-service provider eligible to issue a TFSA. An eligible institution is referred to as the issuer of the plan.
2. You will need to provide your social insurance number and date of birth in order to register.
3. Failure to provide correct information or the provision of incorrect information may cause deregistration of the TFSA and subsequent tax consequences.
4. You may have more than one TFSA but total contributions cannot exceed the TFSA contribution room for the year.
5. Contributors must be residents of Canada.
6. Contributors must be at least 18 years of age. However, unlike RRSPs, there is no requirement to collapse a TFSA at the end of one's 71st year.
7. Only the TFSA holder can contribute to the plan.
8. Accumulated contribution room occurs whether or not a TFSA is opened.
9. It is not necessary to have employment income to contribute, nor do you need to have employment income to accumulate TFSA room.
10. Attribution rules do not apply. For example, if your spouse or common-law partner receives funds from you to place in his or her TFSA you need not be concerned that the funds provided may end up taxable in your hands.
11. Self-directed TFSA's are permissible.
12. Investments that qualify for a TFSA are generally the same as those permitted in an RRSP. Although certain shares of small business corporations are permissible, it is best to speak to your chartered accountant or issuer to ensure that you do not invest in ineligible investments. One major difference compared to RRSPs is that investments in a TFSA must continue to remain eligible after acquisition.
13. Should you decide to contribute to a TFSA in foreign currency the currency would be converted to the Canadian equivalent. Naturally the amount of contribution cannot exceed the annual contribution limit in Canadian dollars.
14. "In kind" contributions are permissible as long as they meet the qualified investment criteria. The valuation will be the fair market value at the time of contribution. If the fair market value exceeds the cost, the difference will be considered a capital gain and must be considered in your personal tax return in the year of disposal. Capital losses on the transfer of "in kind" assets to a TFSA are not deductible as a capital loss in your personal tax filing.
15. The TFSA contribution room is made up of the annual TFSA dollar limit (initially \$5,000 in 2009, indexed thereafter for inflation) plus unused TFSA contribution room from previous years less previous years' withdrawals excluding qualified transfers.
16. The CRA will determine your contribution room based on the information provided by the issuer and will indicate the annual contribution room on your Notice of Assessment.
17. If you do not file a tax return you may still contribute to a TFSA. However, the CRA will not provide information about your contribution room. As such, maintain records of the contributions and withdrawals to avoid overcontributions.
18. You cannot contribute more than your TFSA contribution room in a given year, even if you make withdrawals from the account during the year. (Remember that withdrawals in a year increase next year's contribution room.) If you do so, you will be subject to a tax equal to 1% of the highest excess amount in the month, for each month you are in an overcontribution position.
19. For those who may be concerned as to whether withdrawing funds from their TFSA may cause eligibility problems for the federal income test for

benefits and credits, don't worry; withdrawals will not impact your eligibility requirements.

20. Your Old Age Security (OAS) benefits, Guaranteed Income Supplement (GIS) or Employment Insurance (EI) benefits will not be reduced as a result of amounts withdrawn from a TFSA.
21. For those on Old Age Security (OAS) or for those receiving Guaranteed Income Supplements (GIS) or Employment Insurance (EI), the aforementioned benefits will not be reduced as a result of income earned in a TFSA.
22. Taxpayers receiving the Canada Child Tax Benefit (CCTB), Goods and Services Tax Credit (GSTC), the Working Income Tax Benefit (WITB), or the age credit will not have these benefits impacted by income earned in the TFSA vehicle.
23. Transfers between TFSAs owned by the same individual are not subject to tax or penalty as long as the appropriate forms and procedures are adhered to.
24. Unlike assets in an RRSP, the assets in a TFSA can be used as collateral for a loan outside of the TFSA.
25. Unlike RRSPs, there are no tax implications at death.

Marital or Common-law Breakdowns and TFSAs

In the event of marital or common-law breakdown, amounts can be transferred directly from the account of a former spouse to the other if:

- a) you and your current or former spouse, or current or former common-law partner are living separate and apart at the time of the transfer and you are entitled to receive the amount:
 - under a decree, order, or judgment of a court, or under a written separation agreement;
 - to settle rights arising out of your relationship on or after the breakdown of the relationship.
- b) transferred amounts will not reduce the recipient's eligible contribution room. Since this transfer is not considered a withdrawal, the transferred amount will not be added back to the transferor's contribution room at the beginning of the following year.
- c) the transfer will not eliminate any excess amount in the TFSA.

Tax Savings are Always Worth the Effort

The incentive to save combined with the ability to make tax-free withdrawals suggests the TFSA is a worthwhile vehicle. Should you need more information, give your chartered accountant or financial manager a call. ■

MONEYSAVER

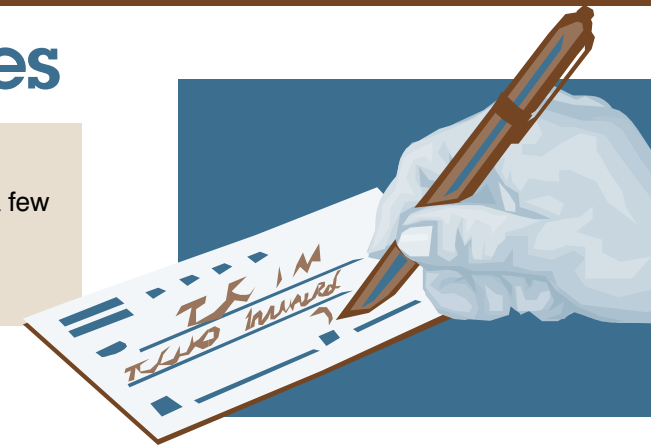
Check Your Cheques

Cheque fraud is a common business problem but a few common-sense precautions can reduce the risk.

But We Paid That Account

Imagine this common scene. Invoices and cheques arrive on the desk of the owner/manager ready for payment. The owner/manager compares the supplier names and the amounts on the invoices and cheques and signs the cheques.

A few weeks later, much to the owner/manager's surprise, the supplier telephones and asks whether there is any reason their invoice has not been paid. After searching the records the owner/manager contacts the supplier and provides details of the payment based upon the cancelled cheque or the electronic transfer record. At this point the owner/manager discovers the



accounts payable department has been duped by a sophisticated fraudster.

Investigation reveals that the bookkeeper received a fax, an email or a telephone call from the supplier asking that the records in accounts payable be changed to a different company mailing address, or bank and bank account number for payments.

Unfortunately, by the time the corporate bank statements are received the fraudsters have cashed the company cheque and emptied the company bank

account. The funds are now gone but the obligation to pay the supplier remains.

That's Not My Signature

Cheque fraud has been around for a long time. Even though more and more payments are being made through electronic transfer facilities, billions of cheques are written each year. The fact that very few of these billions actually undergo human scrutiny, leaves cheque fraud as a continuing lucrative area for white-collar criminals.

Cheque fraud falls into three main categories:

Counterfeit cheques are those drawn on non-existent accounts or accounts set up for the purpose of committing fraud. Businesses can be conned out of supplies by individuals paying for supplies by cheque. By making the purchase on the day before a long weekend, the fraudster has disappeared by the time the cheque is returned from the financial institution. The supplier is out the product and usually has little recourse. Sophisticated scoundrels will even go so far as to set up a dummy company and make small purchases in the company name. The goods are paid for with cash or money orders to build trust. When the time is right a major purchase is made, the goods are picked up, a cheque is written and of course the cheque is returned.

Forged cheques are cheques drawn on legitimate bank accounts but signed in the account holder's name by someone other than the account holder. Because most cheques are cleared electronically without the signature being verified against the signature on file at the originating financial institution, forgery has become easier. A careless owner/manager may have company bank accounts depleted in a systematic and continuous manner through forgery. Cheques are often forged by trusted, long-time employees to obtain money for personal use. A common method is to write a cheque to cash and then charge it to the owner's draw account or to an expense account.

Altered cheques are cheques on which the name of the payee or the amount has been changed. This type of fraud is a bit more difficult to commit since a real issued cheque must be intercepted then altered. Cheque altering is often done by someone in the business with access to payroll- or expense-report cheques. A "1" inserted in front of 120 could enable the cheque to clear for \$1,120. Changes to cheques going to outside entities must involve collusion between a company employee and the person receiving the altered cheque. The recipient would post against the correct amount to accounts receivable and split the remainder with the originator.

Out-going mail may be "scooped" before Canada Post comes around. Envelopes suspected of containing cheques are removed, the cheques taken out and altered to a larger amount and deposited into a bank account with a name similar to your supplier. Cheques from your debtors can also be taken and deposited into a bank account with a name similar to your company name. In either case, the speed of electronic clearing enables the fraudster to disappear by the time you find out. Recovery of funds is impossible.

Protect Your Company

To stop this type of fraud follow up any changes of address with a trusted representative at your suppliers. If the fax, email, or caller provides a confirmation number to call, do not rely on it; you may simply be returning a call to the fraudster. Instead, take down the number and check the data with information on file. It is highly coincidental that a company would change cell phone numbers, bank accounts, addresses and employees all simultaneously. Thus, a telephone call to a trusted contact is the best means of ensuring the correctness of the change.

Never provide high-risk information to any oral, electronic or written communication that asks confirmation of data in your files. Requests for confirmation of date-sensitive, high-risk information (such as banking information, company mailing address, key contact names, or business name), should never be provided unless there is 100% assurance the individual asking for the information is an authorized representative of the company.

A Dozen Ways to Reduce Risk

Protecting your company against cheque fraud means taking a few preventive measures:

1. Use electronic payments such as wire payments, direct deposit and pre-authorized payments.
2. Mail cheques in envelopes that make the contents difficult to identify.
3. Maintain control of unused cheques. Issue cheques to those who need them in batches and have them sign for the range of the sequenced cheques received. Unused cheques should be kept under lock and key.
4. Notify your financial institution as soon as misappropriation is suspected. It has the resources to carry out an investigation
5. Never provide blank signed cheques to even your most trusted employee. If the cheque is lost anyone can put any amount they want in the amount column and make it payable to anyone they wish. Your business will undoubtedly be out the money.

6. Shred all unused cheques for closed accounts.
7. Segregate the responsibilities of employees preparing cheques, paying accounts payable, and doing payroll, from those of employees signing the cheques and reconciling bank statements. Combining these responsibilities in one person creates opportunity to misappropriate funds then cover up by manipulating the records.
8. Ensure prompt account reconciliation and review the reconciliation and the bank account monthly. Question any delays in producing reconciliations.
9. Pre-number all cheques consecutively. If using a computerized numbering system, make sure the new series of computerized cheque numbers agrees with the preprinted cheques. If the number generated by the computer does not agree with the preprinted cheque number, ask questions. Account for all cheques.
10. Never have more than one set of cheques for any one account.
11. Follow up on any old outstanding cheques. Contact the recipient of cheques that are outstanding and determine why the cheque has not been cashed. If the individual/company cannot be located cancel the cheque.
12. Open all company mail, review deposits and personally follow up with any supplier enquiries. Review your on-line bank-statement data on a regular basis looking for unusual or unfamiliar transactions.

Don't Let This Happen to You

Accounts payable and cheque fraud are but two of many means by which unscrupulous individuals can remove funds from your company. When times are tough embezzlement is an easy way for third party and employees to steal from your company. Owner/managers can lessen the probability of loss with increased vigilance for the unusual and active participation in any review of financial matters. ■

TECHNOLOGY

Learning from a Worm

After 15 million PCs have been infected by the Conficker worm, there is much to learn about protecting data.

In little more than a year, as many as 15 million computers have been infected by the Conficker worm. Although that is only a small percentage of the world's one billion PCs, it is a substantial number to be infected by one worm. Conficker infects through a vulnerability discovered in Windows that allows an attacker to gain complete control over a computer. According to security experts, one reason it was able to become so pervasive is that many PCs are operating with unpatched copies of Windows.

Keep It Current

Windows may not be patched to the latest version for one of two primary reasons: the computer cannot download the newest patches, or the user or IT administrator has not opted to download them. Microsoft's anti-piracy solution, Windows Genuine Advantage (WGA), routinely checks the validity of the software licence. If the licence is invalid, the computer is pre-



vented from downloading patches and updates from Microsoft to repair vulnerabilities such as the one exploited by Conficker. Many computers are not kept up to date with the latest patches as a result of either ineffective corporate IT policies or inattentive users. Approximately 30 percent of Windows computers were not protected against Conficker as of January 2009.

Patches Alone are Not Enough

Most malware does not get the amount of attention Conficker has received; Microsoft even offers a free

removal tool. Antivirus software can provide effective protection against malware. However, if a worm such as Conficker is not completely eradicated it may be able to reinfect the system using tricks such as autorun and scheduled tasks to re-execute itself. When Conficker is executed in a PC, it disables anti-virus software, Windows features such as the Windows Update, Windows Security Center, Windows Defender and Windows Error Reporting service, and blocks access to over 100 websites related to security.

Conficker was particularly communicable because it could propagate itself via local networks, the Internet and external devices such as USB flash drives. The worm was also able to perform brute-force attacks against network shares and could gain access via weak passwords. The worm becomes embedded in the operating system and purportedly can lie in wait to receive further instructions from an attacker.

Best Practices

Most computers are likely now patched to prevent infection by Conficker; however, the following best practices will help prevent infection by the next virus or worm.

1. Always ensure your software is genuine and registered. Your PC vendor should provide the original software media even if they have already been "loaded." If the original software media have not been provided, ask why. It is possible to go online to determine whether the Microsoft software you are using is genuine.
2. Ensure your operating system is set to download updates automatically. Be sure the updates are actually installed. Updates are often downloaded then await instructions to be installed. If you have a larger office with a Windows Server environment, consider using Windows Server Update Service (WSUS) to centrally manage patches on all of your computers.
3. Always ensure antivirus software is installed and up to date. As with Windows, be sure the program is configured to update itself automatically and regularly.
4. Data policy should require only company-approved storage or backup devices be used to backup and restore company data.
5. Data that has come in contact with an offsite computer should be scanned for infection before being allowed to be accessed or to reside on company computers.
6. Computers and backup devices should be scanned regularly and simultaneously to ensure they are clean and cannot infect or reinfect clean devices.
7. Internet use should be limited to business purposes and then only with trusted providers. If uncertain as to the trustworthiness of a site, do not visit or download anything.
8. Do not rely on free anti-virus software. Designers with inadequate resources may leave your company vulnerable because they cannot keep up to date. Do not purchase security software from vendors offering a centrally managed "corporate" version.
9. Smartphones, iPods, digital cameras and other devices are all computers and are not immune to infection; they can certainly store infected data.
10. Do not allow unauthorized individuals access to corporate computers.

Protect Yourself

Malware, including worms and viruses are a constant threat that can potentially cause data loss and reduced productivity. If nothing else, Conficker has highlighted the need for business to adapt to the hostile environment of modern computing. Since computers and data will always be vulnerable to some type of infection, give your environment the ability to fend off malicious software. Ensure your PCs are always patched with the latest version of the operating system and applications and that your antivirus software is up to date with the latest definitions. It may be a good idea to review your policies regarding who may use company computers and what devices may be connected to them. ■

The Budding Entrepreneur

Self-employed individuals have been and will continue to be a major force in the Canadian economy.

The future of the entrepreneurial spirit in Canada is secure but the detours on the road to success often cause delays that ruin expectations. Budding entrepreneurs can avoid these detours if they consider the advice of those who have driven before them.

Here are some important things to think about if you are planning to turn that great idea into a business:

1. Incorporate in order to avoid the unlimited liability of sole proprietorships and partnerships.
2. Never underestimate the working capital required to start and maintain a business.
3. Successful businesses must always be prepared to adapt to the changing environment as well as do solid research into location, product line, and customer needs.
4. Obtaining funds to start a business may take three months. Paying off credit cards, lines of credit or bank loans takes years.
5. Hire an experienced bookkeeper who understands business accounting, regulatory compliance such as GST, payroll, WSIB and Employer Health Tax (EHT) as well as the importance of financial data. Without a proper foundation of historical financial data, decisions may be faulty and cost real dollars.
6. Hire a chartered accountant to provide guidance on business transactions as well as corporate and personal taxation issues.
7. Don't purchase expensive vehicles to impress.
8. Comply in a timely fashion with all government requirements and filings.
9. Do not ignore requests from regulatory authorities for information.
10. Ensure your business is adequately insured.
11. Forget about 9 to 5 and consider 8 to 6 the norm.
12. Customers may not always be right – but they provide the revenue that pays your bills.
13. Do not compromise your personal integrity.
14. Learn to listen.
15. Be prepared to compromise.
16. Always have a succession plan. Train more than one individual to perform tasks important to the continuing operations in the event staff is ill, terminated, or retires.
17. Always make payroll on time.
18. Develop mentor relationships with people more experienced than yourself.
19. Make time for those people important in your life.
20. Separate work from play. When the work day is done it is done. Don't take it home or on holidays.
21. Learn to not answer your phone.
22. Learn to understand your financial statements.
23. Maintain financial data on a daily basis. Know what is in the bank, what is owed to the company and what is owing to third parties.
24. Before making major decisions regarding loans, capital purchases or leases, call your chartered accountant.
25. Consider taking a regular salary rather than draws.
26. Understand the terms and covenants of all agreements and know that you can meet them before you sign.



27. Have a shareholders' agreement and ensure understanding of the terms and conditions before signing.
28. Live your life and operate your business within your means.
29. Understand all areas of human resources such as, hiring and dismissal, workers' safety legislation, harassment, maternity leave, vacation requirements, statutory holidays, and labour law.
30. Prepare cash forecasts and worry about them every single day.
31. Find a good bank manager interested in helping your business – not just getting your business.
32. Maintain your company image with personal appearances at trade shows, and local events such as Little League sponsorships or community endeavours such as fundraising.
33. Ensure all contracts and agreements are in the company name.
34. Provide personal guarantees only as a last resort.
35. Provide excellent product or service at a reasonable price.
36. Imbed a code of conduct and behaviour in company policy and ensure that everyone, including owner/managers, follows it.
37. Respect those who work with you because without them your business will not survive.
38. Maintain a working cash reserve that will allow continued operations for at least two months.
39. Collect your receivables as soon as you can.
40. Always have a contingency plan.
41. Always make calculated decisions not unsupported gambles based on hunches.
42. When times are good pay down debt, build a cash reserve or reinvest in the business rather than taking on a mountain of new debt.
43. When times are good establish loan limits with your financial institutions because, when times are bad, no one will want to lend money.
44. Establish internal controls over all facets of the business such as cash, accounts receivable, capital assets, payables, and inventory.
45. Prepare operating and capital budgets and review them at least once every six months.
46. Two weeks of holidays are less expensive than a divorce.
47. Take control of operational routine within your business. For instance, schedule meetings for 10 a.m., approve and sign cheques on Friday, and respond to telephone calls twice a day.
48. Establish a relationship with a lawyer familiar with corporate issues to ensure a full understanding of all agreements and corporate issues that may arise.
49. Know your limitations and hire people smarter than yourself.
50. Believe that you will succeed. ■

BUSINESS MATTERS deals with a number of complex issues in a concise manner; it is recommended that accounting, legal or other appropriate professional advice should be sought before acting upon any of the information contained therein.

Although every reasonable effort has been made to ensure the accuracy of the information contained in this letter, no individual or organization involved in either the preparation or distribution of this letter accepts any contractual, tortious, or any other form of liability for its contents or for any consequences arising from its use.

BUSINESS MATTERS is prepared bimonthly by The Canadian Institute of Chartered Accountants for the clients of its members.

Richard Fulcher, CA – Author; Patricia Adamson, M.A., M.I.St. – CICA Editor.