

INDEX

TAXATION

When is a Business in Business?

MANAGEMENT

50 Ways to Ensure Privacy

MONEYSAVER

10-1-3-11-16-15-20

TECHNOLOGY

Your Business in Your Pocket

A member of **DFK International**

HAMILTON OFFICE
Effort Square
7th Floor
105 Main Street East
Hamilton, Ontario
L8N 1G6

BURLINGTON OFFICE
The Taylor Leibow Building
First Floor
3410 South Service Rd.
Burlington, Ontario
L7N 3T2

Tel.: (905) 523-0000
Fax: (905) 523-4681

Tel.: (905) 637-9959
Fax: (905) 637-3195

website: www.taylorleibow.com

TAXATION

When is a Business *in* Business?

Entrepreneurs excited by the prospect of starting a new business and anticipating a quick startup often purchase assets or make other expenditures far in advance of actual registration or incorporation. The question then arises: “Are expenses incurred before registration chargeable against revenues?”

The answer to this apparently simple question is complicated by a number of factors involving the Income Tax Act and the subjectivity of timing. It should be noted, however, that, because the Act does not provide specific rules dealing expressly with start-up costs, the tax planner must be aware of both the administrative practices of the CRA and the guidance provided in this area by the courts.

The Act indicates that an expense is deductible only if incurred for the purpose of earning income. Thus, if money were spent to earn income, these expenditures are deductible only if it can be shown that the taxpayer was carrying on business in the fiscal period. This means the taxpayer will have to establish the date the business began and be able to show the expenditures were made as a first step to the start of normal operations.



When Does Business Commence?

Establishing the moment when a contemplated business actually becomes a functioning business is a matter of judgement, since “the moment” depends on the determination of when normal operations begin.

It may be fair to assume that a restaurant, for example, has started business before the doors opened, if the lease arrangements are in place, capital assets are

being installed, or the owners are running ads and interviewing for staff. In such a case, the Canada Revenue Agency would want to determine that significant organizational indicators were already in place to support a planned opening date.

If, on the other hand, the aspiring restaurateur spent money only researching the potential of a restaurant at a certain location, it is likely the CRA would consider the expenditures not connected closely enough with actual business operations to be deductible.



Significant Tax Impact

Determining whether expenditures are made in anticipation of an actual business is significant for taxation purposes.

After a business has started, all expenditures fall into two classes:

- Current expenses to be offset against current revenue
- Capital expenditures to be amortized over the useful life of the capital asset.

Amortization is charged as a non-cash expense against the current and future revenue generated by the use of the capital asset. Certain expenditures, such as lawyer's and architect's fees etc., that would otherwise be treated as operating expenses, may be classed as capital expenditures, if they occur before operations commence and are related to the settlement of capital asset issues. They are normally added to the specific capital item and offset along with the original capital cost of the asset against current and future revenue.

The CRA's position is that operating expenses deemed to have been made before the start of business will not be available to reduce taxable income for the operational year. Further, if these expenditures result in a business or non-capital loss, the loss will not be avail-

able to apply forward against subsequent years' taxable income. Thus, the entrepreneur may make expenditures in what are, in effect, after-tax dollars from which neither the business nor the entrepreneur can receive a benefit.

Similarly, if capital expenditures are determined to have been made before the start of business, they might not be viewed as expenditures for the purpose of generating income. Thus, if the business fails before it begins, the entrepreneur will have a loss that may not provide any taxable benefit.

As noted, when a business begins is a matter of judgement. Probably no single factor can be used to establish the inaugural moment. As a result, whether expenditures made before registration or actual commencement of operations should be included as a capital or operating transaction is a subjective decision.

Evidence of intent assists in clarifying not only the time when operations begin but also the timing and allocation of expenditures for financial- and tax-reporting purposes.

Entrepreneurs should meet with their chartered accountant even if merely contemplating a new start-up business to determine:

- The reasonableness of the anticipated time likely to elapse between expenditures and business commencement
- The possibility of timing expenditures to fall within the same fiscal period as the revenue generated
- Capital assets are purchased only for the site and/or business contemplated
- All fees, licenses, and permits are dated, receipted and specific to the site or the industry
- Agreements, or letters of intent are in place for leases, franchises, and/or capital asset expenditures
- Registration is completed within a reasonable time of commencement
- Necessary expenditures such as site-insurance, building permits, etc., are documented and receipted to assist in the allocation to either income or capital

Plan, Plan, and Plan Again

Responsible planning when starting a business will ensure that the entrepreneur can take advantage of the maximum deductible expenses permitted by the CRA while at the same time satisfying investors and creditors.

This article only provides a cursory overview of this complicated topic. If you are even considering starting your own business and may encounter any situation similar to what has been outlined above, consult your chartered accountant before proceeding. ■

50 Ways to Ensure Privacy

The need for business to protect data maintained for clients and employees should rank higher than the need to protect company operational data and / or business secrets.



Individual and business clients demand that data not be shared either intentionally or accidentally. Indeed, business is required to follow the Personal Information and Electronic Documents Act (PIPEDA) that came into full implementation January 1, 2004.

The best security starts with policies and procedures communicated to all employees. Instilling a sense of the importance of security issues into the corporate culture is important not just because security is the law but also because it is good business and recognized as important by all stakeholders. No matter what rules, regulations, or physical attributes may be built into a system, the human element always remains the weakest link.

Your company should review and implement four areas: physical security, data management, staff involvement and management concerns.

Physical Security

1. Provide shredders to each office employee. Ensure all draft data, temporary file-disc backup, handwritten notes, envelopes, etc., are shredded before the staff member leaves each day.
2. All historical files should be secured under lock and key.
3. All historical data, whether for the business or clients, should be shredded on a regular basis by a bonded company. All hard drives and other forms of electronic storage should be erased with a write-over program and destroyed.
4. All laptops, disk, and hardcopy files should be signed in and out by the user with the date, time, and user's name.
5. An information coordinator should maintain a detailed record of all equipment provided to personnel. Equipment should be checked regularly to ensure users have not added new hardware or software that may be used to the company's detriment.
6. Servers should be maintained in an area separated from any work stations. Consideration should be

given to a key-plus security code, or a biometric registration.

7. Information leaving the office, whether hardcopy or electronic, should be provided with a security lock or password and placed in the trunk of the employee's vehicle.
8. If staff is staying at a hotel, consider placing sensitive data in the hotel safe. When and where possible, download encrypted data from the main server before the meeting to eliminate the need to carry the data.
9. Establish visitor protocols. At owner-managed venues, all visitors must either be accompanied by a known employee or should be refused access beyond reception.
10. Laptops and easily moved workstations should be physically secured to lessen the possibility of theft.
11. Workspaces in offices should be configured to prevent access to hardware and defeat the possibility of computer screens being read or photographed by strangers.
12. Determine whether contracts, agreements, patents, formulas, trade secrets and the like should be stored off premise.
13. Administration areas containing company, employee, or client data, agreements, permanent records, business numbers, bank numbers, etc., should be considered off limits to all except authorized management and employees.

Data Management

14. Purge client files of all data not essential to the current project.
15. Do not allow historical data to transfer with current project files. There is little need to have the entire client history at the desktop or transferred to a laptop.
16. Proprietary information should be identified and provided on a need-to-know basis.

17. All data should be maintained on a central server.
 18. All data on the central server should be segregated and classified according to user-based security permissions. For example, contracts, settlements, formulas, or historical data required by regulatory or taxation authorities but also needed for current use should be filed separately at the highest clearance level before being copied to an ancillary device whether a laptop or a flash drive.
 19. All data released should be handled by a single coordinator to ensure the continuity of the information trail.
 20. Updated files to be reentered into the central server for archival purposes should be handled by a single coordinator, who should ensure the data is scanned for viruses before downloading.
 21. If the server is accessible remotely outside the LAN, data transmitted outside the company network should be encrypted.
 22. All computers, whether desktops or laptops, should be equipped with a master password to allow the key administrator to manage the equipment.
 23. A policy should be established to determine whether each client document requires a password or only client files should be encoded. Consider, for example, that it may be possible to protect a spreadsheet but not a word document.
 24. Consideration should be given to the practicality of password protection on all documents. Care must be taken to ensure that necessary information does not become irretrievable because a key individual leaves and no one else knows the password.
 25. All computers should be scanned for viruses on a regular basis. If a virus is discovered, the source should be found and corrective measures taken to avoid subsequent infection.
 26. Individual records should be maintained for all assigned email accounts, computer system-access codes, PDAs, flash drives and communication devices to augment security measures should a person quit or be fired, die, or lose any company device.
 27. Ensure that the latest program updates for operating systems and security programs are installed where required. Do not use pirated software. Maintain a log detailing the program, software version or number, the update date and the hardware the update was installed upon.
 28. All wireless data transmitted should be encrypted. Ensure that the appropriate network keys are in place to ensure your wireless transmissions cannot be intercepted outside the office.
 29. Develop a policy to identify documentation that cannot be communicated over the Internet or by open communication such as a cell phone. Consider, for example, transmission of employee names and SINS as a serious breach.
- Staff Involvement**
30. Employers should provide in-house courses on the need for confidentiality, company policy, and expected protocol in the event hardware or data is lost.
 31. All employees should receive documentation detailing the need for confidentiality. Such documentation should provide guidelines indicating areas off limits, document types not to leave the office, requirements for coordinating passwords with the IT department, etc.
 32. Discussions concerning company business or clients must be handled discretely. Conversations about business matters in restaurants or while travelling on public transportation are a sure means of breaching confidentiality.
 33. There are no circumstances in which company data, operating systems, or client data should ever be loaded to non-sanctioned hardware such as personal computers, client computers, or flash memory.
 34. Staff should be told not to download from the Internet, transfer, cut and paste, import freeware, make modifications to or update existing software on any company property without the written permission of the assigned administrator. (This would include operating program updates.)
 35. Register the serial number, the configuration details and the date of assignment of all equipment on an employee-equipment voucher. The voucher should indicate that the equipment and software is the property of the company and that the employee understands and agrees to return all equipment, software and information upon termination, resignation, sick leave or death.
 36. The loss of any equipment must be reported immediately so the extent and importance of the loss can be determined and any remedial action must be taken, such as calling clients, suppliers, police or company lawyers.
 37. Employees should always carry sensitive data on their person whether they travel by plane, train or bus. Never entrust it to cargo.
 38. When transported in public, equipment must never be left unguarded. Laptops might be stolen; sensitive data may be downloaded to flash memory without the employee's knowledge.

39. All data gathered while out of the office should be backed up at the end of a session. Whenever possible, the day's session should be transmitted to the head-office server. The backup medium must be carried separately from the laptop.
40. All company personnel should be provided with locking cabinets and instructed to store all files at the end of a work day.

Management Concerns

41. Management should learn the principles of records management to understand how to track files from the date of inception to the scheduled date of destruction. These procedures reduce the risk of improperly storing and destroying files and the cost of storage. Regulatory and taxation record requirements especially should be reviewed and documented.
42. Employees entrusted with sensitive data should be subjected to background checks.
43. All clients of a former key employee, sales person or advisor should immediately be informed that a new account representative has been assigned.
44. Confidentiality agreements must be signed by employees annually.
45. Legal advice should be obtained to determine whether employment contracts should include "breach of confidentiality" as grounds for dismissal.

46. Management must maintain ultimate control and security of all passwords. All changes made by the information coordinator must be reviewed, approved and maintained by management.
47. Employees, regardless of position, should not be allowed access to any office equipment if they have been dismissed, quit, transferred or are on extended medical leave.
48. Procedures for recovering equipment, changing passwords, and escorting disgruntled or dismissed employees from the premises must be written out and followed to the letter to avoid loss, theft or corruption of data and hardware.
49. Provide adequate budget to maintain the most up-to-date operating and security systems and train staff to implement and monitor data security.
50. Audit the mandated security measures regularly. Document any issues discovered, and discuss proposed changes with the appropriate personnel.

Data security is everyone's business. Owner managers who are also directors of their companies may be held accountable if it can be demonstrated that appropriate procedures were not in place to reduce the possibility of privacy breaches. Now is the time to review your privacy policy and procedures to be assured your business could not be found negligent through failure to live up to a commitment of confidentiality. ■

MONEYSAVER

10-1-3-11-16-15-20

What would you do if you won a lottery prize in the millions of dollars? Having a windfall of this magnitude is wonderful, no doubt about it, but the resulting change in your life must be managed, especially if you do not have experience with very large investments.

So for those of you who get to be so lucky, here are some tips.

Keep Your Life on Track

Some advisors suggest you put the ticket in a safety deposit box as soon as you know you've won. This gives you a chance to absorb the shock and think



about the effect of this windfall on the life goals toward which you were working for yourself, family and friends. Don't do anything rash such as quit your job, move, or throw aside your established lifestyle. Even very wealthy people choose to work because they enjoy participating in the affairs of this world and do not want to be pointlessly idle. The trouble with having a dream

come true is that you have to find another one to make sense of your future.

Financial Planner

Before spending any large amounts find a financial planner and get a reality check on just what your new-found money can do if spent or invested. Of course, you will probably want to buy a new car and pay off your mortgage or other debts. When the winnings are in the millions, these objectives can be met quite quickly without impairing the majority of the money. The financial planner can review your current lifestyle and your overall net worth, and show you how to achieve financial security.

Consider the amount of the windfall and the rate of return it could provide if turned into an investment portfolio. Think of your current age and seriously consider whether it is financially feasible to wind up your business or quit your job. In the short term the funds may be adequate to support you. But erosion of the principal through unplanned spending could create a crisis down the road when all the funds are gone, you are a lot older and job opportunities are hard to come by when your former contacts have moved on with their lives and you have lost all those years of on-the-job experience.



Taxes

Although the principal amount of lottery winnings is not taxed when received, if it is invested, any return such as dividends, interest, or capital gains, is taxable. It may be worth checking whether the lottery winnings should be claimed by one or more family members to reduce possible future income tax liability. Unfortunately, investment income from lottery winnings is not considered to be earned income for purposes of deductibility as an RRSP contribution. Although most taxpayers may have

no concerns about taxes on their investment portfolios before the win, they may be faced with the possible assessment of an alternate minimum tax. So, before you invest in any tax-saving investment strategies, speak to your chartered accountant.

Debt May Be Good

Paying off the mortgage and other debt is a common consideration for most lottery winners. But, is this really the best strategy? Immediate use of the winnings to pay of the mortgage will reduce the principal amount available for investment to provide a stream of income into the future. If, for example, the mortgage is at 4.5 % and the invested winnings could return 8.0%, paying down the mortgage may actually cost money. That is not to say you should not consider paying off high-interest debt, but, evaluate whether it is better to pay the debt from the investment income or from principal.

Matrimonial Considerations

Before claiming the big prize, winners should seek advice concerning the effect of the dramatic change in personal wealth and income on their marriages and family responsibilities. Consideration should be given to the impact of sharing the windfall, what may happen in the event of matrimonial breakdown, child support payments, etc. For example, Federal child Support Guidelines require the non-custodial spouse to pay according to their means. If you have just become a big winner and your income has jumped significantly as a result, you may be facing a sharp increase in your monthly child support payments. Understanding the legal issues beforehand allows these issues to be resolved while the financial interests of all family members are protected without the need for costly litigation in the event of matrimonial difficulties, death, or unforeseeable legal proceedings.

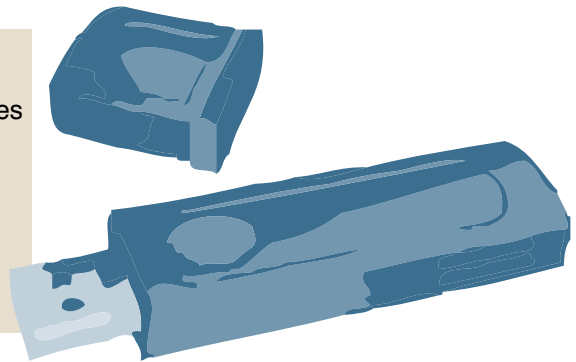
Sharing

To share winnings with family members, donate to charities, or invest in a close friend's business are wishes often expressed by winners. Such generosity is certainly a wonderful personal attribute, but before giving in to this impulse, be aware of the effect of the reduced principal on your future income. Talk to your financial planner about investing the principal and distributing after-tax earnings each year or reinvesting the income from the original investment then, ultimately, distributing out of your portfolio income. This income and capital-distribution approach will protect your future as well as satisfy the innate desire to "share the wealth" or help those in need.

Windfalls, whether from games of chance, inheritances, or fortune in business or the stock market are usually once-in-a-lifetime events. Regardless of the source of your good fortune, ensuring that it lasts for your future enjoyment requires thoughtful management. ■

Your Business in Your Pocket

Everyone who takes a laptop out of the office or completes a desktop task must back up the data to ensure that, if the hardware crashes, goes missing, or the information gets corrupted, the hours of hard work are not lost.



More individuals now use USB flash drives as a secure, portable alternative to storing data on the local hard drive of a computer. Whether one uses the flash drive to work on data, run operating programs, or store email, contacts, etc., there is a growing realization that flash drives are the future of memory. Indeed, the goal of flash drive developers is to create hardware that will eliminate the need to have memory built into computers. The future computer may be just a tool for input and transmission.

The reasonable price has made these little sticks ubiquitous and indispensable to anyone needing to retain or transfer data. Because they contain no moving parts, flash drives are highly durable and reliable.

Although it is impossible to prevent information loss completely, flash-drive technology is now available with encryption to significantly reduce the risk of unauthorized access to the information. Manufacturers offer drive capacities ranging from 1-to-8 GB using simple encryption methods that rely on third-party security software or the host operating system. This level of security keeps your data safe from anyone curious to find out what's on the stick. However, if you need stronger encryption, more secure flash storage is available.

Here are some of the security features accompanying this new technology:

- Tamper resistance that meets validation requirements set by the Canadian government

- The encryption is built into the flash drive and not the host. Thus, the password created when the unit is initialized stays in the unit
- Limited password attempts. Once the threshold is reached, the unit destroys all information
- Any attempt to access the unit's mini circuits causes destruction of all information
- Forget your password? New units have a built-in digital certificate that matches the registration and password stored at a secure server
- Biometric sensors capable of using the fingerprints of multiple individuals combined with encryption codes to access data

The current GB size limits the amount of data or operating systems that can be placed on a USB flash drive but should be sufficient for most small businesses with normal business applications and data-file size. At a price starting at \$80 and peaking around \$300, these units are a positive alternative to other storage media because they provide not only storage but also the comfort of knowing that client, company and staff information cannot be compromised. ■

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.