

INDEX

VOLUME 18, ISSUE 2
April, 2004

TAXATION
Salary, Dividends, Bonuses

MANAGEMENT
The New Privacy Rules

TECHNOLOGY
RFID for Security and Control

MONEYSAVER
Misappropriation

TAXATION

Salary, Dividends, Bonuses

Minimizing corporate and personal taxes is one of the many challenges of running a small business.



For owner/managers of small businesses, one of the benefits of incorporating is that the income of the corporation is entitled to low tax rates as a result of the small business deduction. With this, the initial combined federal and provincial rate of tax on active business income ranges from 16% to 22% across Canada as compared to the owner/manager's personal income tax rates that could range up to 49%.

The low corporate tax rates allow a business to grow. However, they also provide planning opportunities in determining the remuneration for the owner/manager since, even at the lower levels of the personal tax brackets, the personal tax rates are higher. For the owner/manager who leaves the after-tax corporate profits in the corporation, this results in a deferral of tax. With proper planning, this tax deferral may be substantial.

Federal Small Business Deduction

A Canadian-controlled private corporation (CCPC) that meets certain qualifications can claim a corporate tax reduction, called the small business deduction. Depending on the corporate year-end in 2004, the small business deduction applies to active business income up to \$225,000 to \$250,000. For example, a corporation with a March 2004 year-end the small business deduction would be \$231,216 (the 9 months in 2003 at \$225,000 and 3 months in 2004 at \$250,000).

The good news for owner/managers is that the federal small business deduction is further increasing to \$300,000 for the part of the year that ends after 2005.

All corporations that are associated must share the benefits of the small business deduction.

Provincial Small Business Deduction

Most provinces also have a small business deduction and some provide additional relief on active business income up to \$400,000.

Dividends versus Salary

Theoretically, the Canadian tax system is designed so that when business profits, which have been subject to the low rate of tax, are withdrawn from the corporation in the form of dividends, there are no additional tax savings or costs when compared to withdrawing the profits in the form of a salary. However, in practice, there is actually a tax savings in many provinces if the business income is left in the corporation, taxed at these low rates, and withdrawn as dividends, either in the current year or in a subsequent year. If the owner/manager were to draw these amounts as salary, the applicable personal tax would be higher and result in less after-tax funds.

Offsetting Business Income that Exceeds the Thresholds

If business income exceeds the thresholds for the small business deductions, then the corporation is subject to the higher rates of corporate tax of up to 41%. As a result, the tax advantage of taking dividends usually disappears and the owner/manager's best option becomes salary. Since, the higher corporate tax rates leave less after-tax income in the corporation to distribute as a dividend, the cost is higher.

In some cases, the higher tax rates are offset by the deferral of not paying the additional personal tax currently. For instance, if business income is left in the corporation and taxed at rates lower than the incremental rate that the owner/manager pays, then there is a deferral of tax. As the owner/manager is reinvesting this deferral in the business, it grows. If this income is left in the corporation long enough, the growth resulting from the deferral will offset the additional tax cost. In some cases, a couple of years is sufficient for

the deferral to be beneficial. In other cases, it can be a very long time. In these latter cases, reducing corporate profits to the small business deduction limits is usually the best option.

Leaving After-tax Income in the Corporation

When considering whether to leave after-tax income in the corporation, the owner/manager usually makes the assumption that it will be withdrawn in the future in the form of dividends. However, many owner/managers may decide to never withdraw these earnings, opting instead to use them to grow the business. Ultimately, they plan to reap the benefits of these earnings through an increased selling price when they eventually sell the corporation.

Since 2000, the effective rate of tax on capital gains is less than the rate of tax on dividends. This increases the benefits of leaving earnings in the corporation. If the \$500,000 enhanced capital gains deduction is available, these benefits are even greater.

Bonuses

Where business income is taxed at the high rates and there are no benefits to deferring the earnings in the corporation, reducing corporate income to the small business limits is advisable. One option is having the corporation pay a bonus to reduce the earnings. These bonuses are often set up at the corporation's year-end and are paid later.

In order for the bonus to be deductible to the corporation, there must exist a legal liability at the year-end that gives the owner/manager the right to enforce the payment of the bonus. In addition, the bonus must be paid within 179 days from the year-end of the corporation. If it is paid after the 179-day period, the bonus is not deductible in the year when it was accrued but rather is deductible in the year it was paid. In the latter case, the bonus would not serve the purpose of reducing corporate income in the earlier year.

A bonus may also provide a tax-deferral for the owner/manager if it is not received until a subsequent year. For instance, if the corporation has a July 31, 2004 year-end and the bonus is paid 179 days thereafter, that is, on January 26, 2005, the bonus would be 2005 income of the owner/manager.

Sometimes large payments of bonuses cause cash flow problems to the corporation, which are solved by the owner/manager lending the after-tax amount back to the corporation. In these cases, consideration should be given to having the owner/manager charge interest on the loan. The receipt of interest, instead of a higher salary, may be a better tax planning strategy in those provinces that have payroll taxes.

Weighing the Other Considerations

There are many other considerations in deciding whether to pay dividends instead of salaries. These include:

- Ensuring there is enough earned income to maximize RRSP deductions. To claim the maximum RRSP deduction in 2005, of \$16,500, the owner/manager will need to have earned income in 2004 of \$91,667.
- The benefits of income splitting with other family members who are shareholders but are not active in the business.
- The implications of provincial payroll taxes.
- Ensuring Canada Pension Plan (or QPP) benefits will be maximized at retirement.
- Clearing shareholder receivables to ensure there are no negative consequences because of the shareholder loan rules.

There are many issues to review in determining what is the optimal mix of salary and dividends and when is it beneficial to pay bonuses. Your chartered accountant can help you consider the various options and implications and advise you on the most advantageous tax planning strategy for your particular circumstances. ■

The New Privacy Rules



Privacy is a significant concern to Canadian consumers. Numerous polls and surveys have identified fears about privacy as one of the major inhibitors to the growth of electronic commerce in Canada.

In light of these concerns, the federal government enacted the *Personal Information Protection and Electronic Documents Act* (PIPEDA). As at January 1, 2004, the privacy rights of all Canadians are protected in one of two ways: by federal legislation or by provincial legislation that is “substantially similar” to the federal legislation.

This article provides a brief overview of the privacy rules and some of the key requirements for compliance.

Privacy Rights and Obligations

The PIPEDA establishes new rules to recognize the privacy rights of individuals with respect to the collection, use, disclosure and retention of their personal information. The rules also recognize the obligations of organizations to protect personal information in a manner that a “reasonable” person would consider appropriate under the circumstances.

Most organizations regularly collect, use and sometimes disclose personal information. Customer or client files will often contain information such as age, name, ID numbers, income, marital status, investment holdings and other personal information.

Under PIPEDA, organizations must now obtain an individual’s consent when they collect, use or disclose an individual’s personal information. Compliance is to be monitored by the

Privacy Commissioner of Canada (“Commissioner”) who acts as ombudsman and hears complaints under the new law. The Commissioner may, with reasonable grounds, audit the personal information management practices of the organization and make recommendations.

The Act gives protection to whistle blowers and the Commissioner is required to follow up on any alleged breaches of the law or make a formal complaint. Complaints should not be taken lightly. A person is liable to a fine of \$10,000 on a summary conviction or up to \$100,000 for an indictable offence.

Complying with the Privacy Rules

In responding to the requirements of the privacy legislation, owner/managers have been ensuring that all employees are familiar with the requirements of the Act, establishing privacy policies and evaluating their systems to identify those that need to be changed. Much like a system of internal control for financial information, there should be a system of controls to ensure that the organization’s privacy policies are appropriate and are met.

Generally the requirements of PIPEDA are to:

- Satisfy customers and other individuals that their personal information is being protected, and
- Explain to them why the information is being collected.

Note that although PIPEDA does not currently extend to employees’ personal information, this is a requirement under some of the provincial legislation. Companies who fall under the jurisdiction of PIPEDA may wish to extend the scope of their compliance to include employee information as well.

Your Organization’s Privacy Procedures and Policies

The following lists some of the requirements your organization should address in its privacy procedures and policies:

- **Collecting Personal Information**
The organization needs to identify the reasons for obtaining personal information before it is collected and to document the purposes for which it will be used.
- **Obtaining Consent**
The organization must obtain the consent of its clients or customers prior to collecting, using or disclosing their information.
- **Limiting the Use, Disclosure and Retention of Personal Information**
Personal information on file must only be used or disclosed for the purpose for which it was collected, unless the individual consents, or the use or disclosure is authorized by the Act.
- **Protecting Personal Information**
Sensitive personal information must be protected against loss, theft or unauthorized access.
- **Providing Openness and Accountability**
The organization should inform its customers, clients and employees of the existence of its policies and practices (including the complaint process) that are in place for the management of personal information.

CICA’s Online Privacy Resource Centre

The Canadian Institute of Chartered Accountants (CICA) has prepared a Privacy Package of resource materials to help organizations comply with the PIPEDA requirements. These practical privacy-related resources can be downloaded free-of-charge from the

CICA's Online Privacy Resource Centre at www.cica.ca/privacy. The official text of the Act and other information can be found on the website of the Office of the Privacy Commissioner of Canada at www.privcom.gc.ca

The CICA Privacy Framework, a valuable privacy tool developed by the CICA in cooperation with the American Institute of Certified Public Accountants (AICPA), is also available from the CICA's Online Privacy Resource Centre. The Framework can

be used by organizations to guide and assist them in implementing a privacy program. It incorporates concepts from the PIPEDA as well as from significant international privacy laws and provides objective and measurable criteria for evaluating an organization's privacy policies, procedures and controls. In supporting the Framework, Ontario's Privacy Commissioner Ann Cavoukian stated, "A new privacy tool developed by the Canadian Institute of Chartered Accountants will provide valuable assistance to businesses in complying with privacy laws."

Get Professional Advice

The above is a very brief overview of the privacy principles your organization should now have addressed and have in place. As PIPEDA is a complex piece of legislation, be sure to seek the professional advice of your legal counsel and your chartered accountant. Your chartered accountant can provide a range of services with respect to privacy, such as guidance on privacy control systems and value-added privacy services. ■

TECHNOLOGY

RFID for Security and Control

Radio frequency identification (RFID) is a growing area of automatic identification and data capture with several applications in transportation and distribution, product identification, carrier identification, security and access control and animal identification.

Many consumers and businesses are already familiar with some of the RFID tracking and access applications. For over a decade, RFID has been used for toll collection, inventory control, building security and library systems. Because it can be used to track moving objects, it is well established in areas such as livestock identification and automated vehicle identification systems. New generation, lower cost systems with more storage capacity and other technological advances are rapidly making RFID available to a wide range of industries for various applications.

A basic RFID system consists of a reader (or interrogator), antenna and RFID tags or cards (transponders) that carry the data. The RFID tags are embedded within or on objects. The tag receives a low-power radio signal that is transmitted from the reader through its antenna that powers the tag's integrated circuit (chip) to "talk" with the reader, verifying and exchanging data. The reader can then send this information to a computer for processing and management. Encryption keys and validation procedures ensure the authenticity and accuracy of the information.

Companies use the less costly low frequency systems with short reading ranges for security access, asset tracking and animal identification. The more costly higher frequency systems are used in applications such as toll collection and railroad car tracking. Not only does the RFID system improve security, but it also increases the accuracy and reliability of the company's inventory data.

Because the tags do not need to be visible in order to be read, they can be hidden in boxes and other containers to

provide an extra measure of security for valuable inventory and equipment. The tags can even be read through fog, snow, ice, paint and other challenging or hostile conditions where bar codes or other optically read technologies would not work. For example, RFID systems can identify and track high value units moving through an assembly process, such as painting or baking.

The RFID system's ability to improve inventory management processes and demand planning, deter theft, reduce costs and enhance customer satisfaction is rapidly making this technology a competitive advantage for a wide range of businesses. In the retail sector, some major players are requiring their suppliers to RFID tag all cartons and pallets by the year 2005 so they can more effectively track inventory shipments, pallets, cases and high-end inventory.

While it is unlikely to replace barcode labels, RFID tagging is worth investigating if your business needs to improve its systems for identifying and tracking high value items. ■

Misappropriation

While you are taking care of business, what are the people who are taking care of your business doing?



Theft and fraud can happen in any organization but it is a lot easier when the company has poor internal controls or dubious ethical values.

Some of the frauds commonly perpetrated in small businesses include the misappropriation of funds, expense account fraud, cheque forgery, manipulation of cheques, purchases for personal use, kickbacks or manipulation of financial statements to reach a bonus target. In addition to losses instigated from within the organization, fraud can also be committed against the company by suppliers and customers. For example, a supplier may submit false or duplicate invoices or overcharge for services or goods. A customer may deduct false credits to reduce the amount owing.

As a first step, make sure you are familiar with the warning signals that could flag the misappropriation of funds or assets. Take time to review your processes, controls and security measures and create or amend policies, procedures and responsibilities where necessary.

Here are some security measures that can help prevent losses.

Computers

- Install firewalls, passwords, and security software programs to deter unauthorized access to computer data and programs.
- Install a security system that logs each individual's access to programs and databases.
- Establish master passwords for all systems. Never provide this information to any employee. Regularly review existing passwords and users and regularly change your master password.
- Ask your computer specialist to regularly review desktop computers, laptops and servers to ensure only authorized software is being used and the virus scanner and other security measures are current and operating.
- Ensure computer terminals cannot be accessed when employees are absent from their desks.

Physical Security

- Attach computer alarm chips/tracking chips to all high-end inventory and capital assets.
- Limit access to sensitive office and plant areas with swipe cards and password technology.
- Secure computers to desks.
- At the end of each day, ensure all cheques, cheque writing machines, and security cards are locked in filing cabinets or secured in an office safe.
- Limit access to main entrances. Require all guests to register and wear a guest nametag.
- Have employees sign out expensive equipment such as laptops or power tools and track that these items are returned.
- Quickly scan the mail before it is distributed for processing. Be alert to any unusual correspondence or invoices.

- Shred documents that are no longer needed before disposal.
- Maintain up-to-date records of all equipment, including serial numbers and location. Once in a while, verify where they are.

Banking

- Each month, reconcile and review bank statements along with details of term deposits, overdrafts, returned items, special charges and deposits. Stale items on any reconciliation bear watching.
- Track short-term investments (such as 30-day term deposits) that are deposited into the account to ensure that amounts are not substituted as accounts receivable.
- Do not write cheques to cash.
- Do not provide employees with a company PIN for cash withdrawals or other transactions. Do not ask assistants to cash your personal cheques.
- Do not sign blank cheques for future purchases.
- Review payroll direct deposits to ensure legitimacy of the employee or contractors.
- Maintain security over all cheques. Keep records of the quantity of cheques ordered and the numbers. If software systems assign cheque numbers, make sure that the software number agrees with the physical cheque number. If the numbers are not the same, account for the missing cheques (electronic or physical).
- When cheques are voided, do not destroy them; file them with cancelled cheques. Excessive voids, credit memos or late charges may mean that an accounts receivable is delinquent because payments are being received and diverted elsewhere.

- Issue pre-numbered receipts for all cash purchases, including the customer's name, items or service purchased and the payment received. Make cash deposits daily.
- Be alert for missing or altered documents. With today's photocopying technology, copies can easily be mistaken for originals.
- Review and take immediate action on any enquiries from provincial and federal authorities regarding sales taxes, health taxes, employee deductions, and WSIB or EI payments.

Signing Authority and Limits

- Establish signing authority limits for employees in areas such as operating lines, payroll, credit cards, purchase orders and customer credit. Require two signatures for amounts in excess of these limits.
- Review purchases and sales regularly. Watch for unusual amounts that may indicate the costs have been split to circumvent authorized limits.

Staff

- Personally authorize all hiring, dismissals and any changes in remuneration, benefits, etc.
- Limit access to payroll data to specific individuals.
- Review employees' and contractors' time submissions. Ensure they are reasonable in the circumstances. Make surprise visits to job sites. Talk to your customers to determine the working habits of employees or sub-contractors.
- If an employee resigns or is terminated, advise all staff and ensure that keys, security cards, credit cards and other company items are returned promptly. Remove the individual's passwords from all computer systems and other communication systems

and notify relevant organizations that the individual is no longer an employee.

- Ask sub-contractors to sign non-competition and confidentiality agreements.
- Rotate job responsibilities. Be wary of employees who rarely take holidays or deal directly with only one individual and are reluctant to deal with others.

Expense Accounts

- Review all expense submissions. Authorize reimbursement only where proper documentation is provided. Ensure that duplicate invoices are not submitted or credit card statements are not used to support expenses incurred (unless original source documents are attached). Watch for any inappropriate charges to expenses.
- Maintain reports on expense breakdowns by individual and cost centre on a long-term comparative basis. Review spending patterns and follow up on unusual spikes or drops in expense report submissions.
- Review car expenses related to personal use and monthly vehicle allowances. Ensure employees keep automobile logs in which they record the date, distance and purpose of trips.
- Review your own draw account regularly to ensure that unauthorized expenditures are not being charged to your account.

Customers

- Review and approve the granting of credit to new customers and the extension of credit to existing customers.

- Regularly review the accounts receivable listing and contact customers who have overdue accounts. Enforce a COD policy for delinquent accounts.
- Review all outstanding accounts and actions taken. Approve the write-off of amounts that cannot be collected.

Suppliers

- Review and approve all new suppliers and credit limits.
- Regularly review accounts payable for new suppliers, noting any unusual amounts or purchases and suspicious addresses or telephone numbers.
- Approve and review all new contractors. Be sure to request the appropriate references, bonding and insurance details.
- If ordering and paying online, ensure encrypted data transfer protocol is in place.

Inventory

- Conduct regular inventory counts, both in total and on a random item basis and reconcile the data to perpetual records.
- Secure all inventory areas with traditional locks, swipe cards and other security measures.
- Consider installing video surveillance in the yard, shipping and warehouse areas. Regularly review the tapes.

Reducing the opportunity for the misappropriation of funds and assets is an ongoing responsibility for everyone in the company. It is also a very important consideration when modifying or developing business processes and procedures. Talk to your chartered accountant about how you can improve your internal controls and oversight procedures to protect your business from losses through theft or fraud. ■

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; Kathleen Aldridge, B.A., Dip. Ed. – CICA Editor.