

INDEX

VOLUME 18, ISSUE 1
February, 2004

TAXATION
Late Payroll Remittances

MANAGEMENT
Travel Smart

MONEYSAVER
Reducing Energy Costs

TECHNOLOGY
Managing Your Computer Systems

TAXATION

Late Payroll Remittances

Prior to changes announced this past June, the penalty structure for employers who submitted their payroll remittances a few days late were quite onerous.



As an employer, you are responsible for deducting and remitting Canada Pension Plan (CPP), Employment Insurance (EI) premiums and income tax from amounts you pay to your employees along with your share of these withholdings to the Receiver General. In Quebec, employers must remit provincial deductions and contributions to the Quebec Pension Plan (QPP) to the Minister of Revenue of Quebec.

For the most part, employers voluntarily pay their payroll remittances on schedule. However, if they were just a few days late, the previous flat penalty rate of 10% was viewed to be overly punitive.

Penalties Now Graduated

As of June 2003, the Canada Customs and Revenue Agency (CCRA) administratively replaced the flat penalty rate with a system of graduated penalty rates for late remittances. In response to ongoing discussions with employers and associations such as the

Canadian Payroll Association, the CCRA revised the penalty structure to focus on good performance while deterring employers who chronically remit late.

The current penalties for remitting late are:

- 3% for remittances that are late 3 days or less
- 5% for remittances that are 4 or 5 days late
- 7% for remittances that are 6 or 7 days late, and
- 10% for remittances that are 8 or more days late.

Failure to Remit or Pay

However, the penalties for failing to deduct or withhold have not changed. An employer who fails to remit or pay as and when required may be subject to a penalty of 10%. A 20% penalty applies where the failure to remit is made knowingly or under circumstances amounting to gross negligence.

Director's Liability

If a for-profit or not-for-profit corporation fails to deduct, withhold, remit or pay amounts held in trust for the Receiver General (CPP, EI, income tax and GST/HST), the CCRA may also hold the directors of the company at the time of the failure personally liable to pay the amount due, including penalties and interest.

Payment Must be Received by the Due Date

A remittance is not considered to have been paid until such time as the Receiver General receives it. If you mail your remittances, be sure to post them long enough in advance to ensure the Receiver General receives them by their due date. If you make your remittances at a financial institution, they are considered received on the date that the funds are electronically transferred to the CCRA.

If you use an automated teller machine (ATM) to make your remittances, be sure to allow time for the financial institution to process the payment. While the financial institution debits

your account as at the date of your transaction or the next day, the CCRA does not view an ATM receipt as proof of its having received the payment by the due date.

If you are concerned about the processing time, you can make your payment directly at a Tax Centre. Whether you make your payment at a financial institution, an ATM, or at a Tax Centre, the CCRA must receive it on the date that it is due.

If you are a regular remitter, generally you must remit your deductions on or before the 15th day of the month following the month that you made them. If the 15th is a Saturday, Sunday or a statutory holiday, your remittance is due on the next business day. For corporations that are eligible for quarterly remitting, payment must be received on or before the 15th day of the month immediately following the end of each quarter.

Threshold 1 and 2 remitters (that is those employers who had an average monthly remittance two years ago equal to or more than \$15,000 and less than \$50,000 and those who had an average

monthly remittance two years ago of \$50,000 or more) have their own payment date schedules. Note that Threshold 2 remitters must make their remittances at a financial institution.

Monitor Payments Carefully

It is important to monitor the company's payroll remittances and GST/HST payments carefully to ensure the company and its directors are not liable for late penalties and interest. Your chartered accountant can help you review your accounting system to ensure the company makes its remittances by the due date.

You can print or download more information about the dates for remitting deductions, the required forms and some helpful publications by visiting the business section of the CCRA website at www.ccra.gc.ca or you can obtain this information by visiting your local tax services office. The website also provides the addresses of the Tax Centres for making your payments. ■

MANAGEMENT

Travel Smart

Flight delays, stringent security checkpoints and travel alerts are making every traveller keenly aware of the importance of travel planning, preparations and precautions.

Here are some practical tips that can help protect your safety, health and valuables and reduce the likelihood of problems when you are travelling for business or pleasure.

Travel Itinerary

Provide your business associates and family with a copy of your travel itinerary, including the details of your flight number, departure arrival times and contact information. If you have not previously booked a hotel at your destination, contact your office and home with details on arrival.

Travel Documents

Your passport is your most valuable document. Keep a copy of your passport number in a safe and separate place in your carry-on or luggage. Leave a photocopy of your passport in a secure place at home or with a relative or friend.

Photocopy your traveller's cheques, airline tickets, and other travel documents. Carry one copy with you separate from the originals and leave a copy with a relative or friend. You should also make a list of the emergency contact telephone numbers should you need to report your debit or credit card is lost or stolen. Do not

include your card account numbers on the list that you will carry and certainly never write down your PIN numbers.

Prohibited Items

Airlines now prohibit many items to be carried on-board in your carry-on luggage or packed in your luggage that is checked in. Take a close look at the items you carry in your pockets, briefcase and grooming kit. While it is obvious you should not carry or pack a pocket knife, letter opener, scissors, nail file or similar items, you may be surprised at the items that are included on the airline's prohibited list.

Ask your travel agent or airline to provide you with a list of items that are permitted or prohibited in your carry-on or checked baggage. Some items may be allowed in your checked baggage but not your carry-on.

If you bring a prohibited item to the checkpoint, you may be detained and prosecuted depending on the jurisdiction. At the very least, you will be asked to dispose of the item. Before you leave for the airport, double check the contents of your pockets and bags, particularly carry-on luggage, to ensure you have not inadvertently packed a prohibited item.

If you want to reduce your wait time at the security checkpoint, carry as little as possible with you and avoid wearing anything that contains metal. Be aware of the security procedures that may apply to certain items. For example, if you need to carry a laptop or other electronic equipment, you may be asked to turn it on or open various components. Know what is in your carry-on as well as your checked-in luggage as you may be asked to provide details.

Get as much information as possible from your travel agent and other sources about the destination, especially if you will be travelling alone. There may be laws and regulations you need to be aware of, particularly if you are carrying commercial products or course materials.

Identification Tags

Remember to put identification tags both inside and on your suitcases and carry-on luggage including your laptop. Laptops are one of the items that people most frequently forget at checkpoints and when leaving an aircraft. When tagging your luggage, consider using only your last name and first initial along with your business address and telephone number rather than your home information.

Never leave your luggage unattended and of course, never accept the responsibility for someone else's luggage.

Be prepared in case your luggage is lost or delayed. If you are carrying two suitcases, make sure each has a full complement of business and other attire. Persons travelling with a companion may wish to consider packing some of their clothing in each other's luggage.

Health and Medical

Keep in mind that the healthier you are before the trip, the more likely you can reduce the effects of jet lag. Several days before the trip, adjust your sleep schedule, take stretch breaks and drink lots of water. Plan to eat only light meals on the day of the trip.

For out-of-country trips, be sure to purchase the appropriate medical coverage through your travel agency or financial institution. Your provincial health plan may provide some coverage but there may be caps on amounts and other restrictions. Look for a travel insurance plan that includes 24-hour, toll-free telephone assistance and pays directly and immediately to the medical provider. If your credit card includes travel medical coverage, be sure to read the fine print to determine if it is sufficient.

If you have ongoing medical problems, it is advisable to have your physician prepare an explanatory letter to carry along with your medications. You should also consider wearing a medical alert bracelet in case of an emergency.

Your travel agent can inform you if your destination requires you to have certificates of vaccinations before you are allowed to enter.

Airports

Arrive at the airport well before your flight time, usually a minimum of two hours before the flight. Whether you are taking a domestic or out-of-country flight, be sure you have all your travelling documents and receipts with you.

The security checkpoints are for everyone's benefit. Be patient. Line-ups and thorough screenings are the norm today.

On Arrival

Orientate yourself on arrival. Ask the concierge or other hotel staff to point out the location and best routes to businesses, restaurants and the Canadian Embassy or consulate.

Store your valuables, including your passport, in the hotel safe or wear a money belt to keep these secure. Be observant at all times to reduce the chances that you will become the victim of a pickpocket or thief. Keep a low profile. Dress down. Expensive jewellery and clothing could make you a target for theft.

When using a credit card, do not let the card out of your sight and ensure it is returned to you afterwards. Only use your debit card at ABMs that are globally branded or located at a branch of a major financial institution.

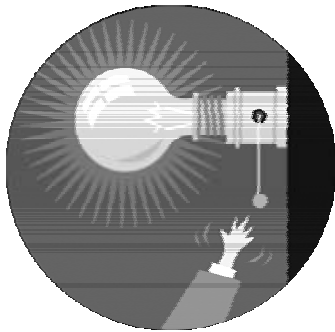
Travel Smart

Whether you are travelling for business or pleasure, plan your trip carefully, take precautions to reduce your risk exposures, and have a back-up plan in case of emergency. Your knowledge of procedures and regulations along with your careful preparations can help ensure you have a productive and safe trip. ■

Reducing Energy Costs

With energy costs

continuing to rise, owner/managers and employees need to work together to reduce consumption while at the same time lessening the impact on the environment.



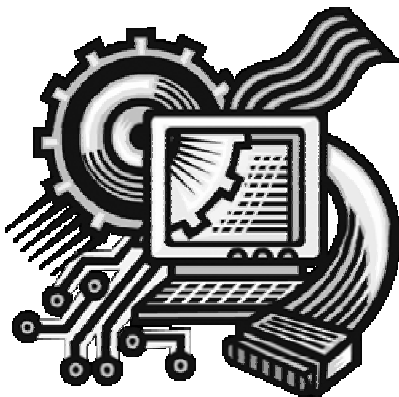
As a starting point, here are some simple practices that can help you and your employees reduce the company's overheads for electricity and heating.

- Close office doors to areas that are not in use. If possible, reduce the airflow or heat to these locations.
- Turn off the lights when they are not needed.
- Use spot heaters to warm areas that tend to be cold rather than turning up the thermostat to heat all areas.
- Replace traditional filament light bulbs with energy-efficient bulbs or fluorescent lighting. Not only will this reduce electricity costs but also the bulbs last up to 12 times longer.
- Use desktop lamps for extra lighting.
- Do not habitually turn on equipment when first arriving at work. Save energy costs by turning on the equipment when it is needed.
- If the company provides staff with outdoor plugs for their car block heaters or inside car warmers, consider the feasibility of installing a timer to turn the power on an hour or more before staff depart rather than having vehicles plugged in all day.
- Check windows for drafts and air leakage. A low cost energy-saver is to tape polythene across window frames where needed.
- Open curtains or blinds to allow as much light in as possible during the day. Close blinds or curtains at dusk to prevent heat escaping through windows.
- Examine your entranceway to determine whether heat is escaping when the main door is opened. Consider improving or adding an enclosure to reduce heat loss.
- If you do not have programmable thermostats, encourage staff to turn the heat down one or two degrees when they are the last ones to leave the premises. Lowering the heat is particularly cost-effective on weekends and holidays.
- For high consumption applications, contact your utility provider and determine the cost advantages of scheduling some processes after peak hours or on weekends.
- Monitor energy usage and analyze any increases in consumption. A review may alert you to methods that need to be changed or equipment that needs to be replaced with energy-efficient models.
- Get energy-saving advice from your utility provider and schedule an energy review of your premises.

These tips can help you save money on your electricity and heating at your business as well as at your home. Encourage your employees to make a conscious effort to reduce energy costs. Post friendly reminders to help make all employees aware that their energy-conserving efforts can make a difference. ■

Managing Your Computer Systems

Are your employees aware of your company's policies for the use of company desktop and mobile computers, software and other computer equipment? Does your company have up-to-date records of all computer hardware, software applications, versions and licensing agreements? Who maintains these records and how frequently are they reviewed and updated?



While computers enable us to work faster and smarter, their widespread use also creates certain risks, including risks of security to information and equipment and potential legal liability. Establishing clear company policies on computer usage and keeping careful records of your hardware and software are good business practices for ensuring your computer systems are continuously available. These measures also help you guard the privacy and confidentiality of your company's competitive information and the data entrusted to you by customers and employees.

Company Policies and Guidelines

In order to maximize the benefits and minimize the risks associated with the use of computer networks and the Internet, every company should establish policies and guidelines for all users. These should also be periodically reviewed and updated to reflect changes in systems and processes.

Generally, a company's computer policies address:

- Use of hardware (desktops, laptops and peripherals) and software.
- Access to, and use of, the Internet and e-mail.
- The viewing, accessing and downloading of text, image, video, sound and software from the Internet.

If your company does not already have these policies in place, there are many books and Internet resources that can help you develop clear company policies and guidelines for computer usage.

Make sure every employee is aware of the importance of the company's computer policies and guidelines, and ensure all employees comply.

Systems Administrator

While it is every employee's responsibility to comply with the company's computer policies, it is important to assign the authority for reviewing, managing, purchasing and installing new hardware and software to an appropriate individual. As the systems administrator, this person should be the only person authorized to:

- Install or remove software, make software changes, and add computers and peripherals to the company system.
- Maintain application change controls, as the ability to change a program is also the ability to create and alter data.

Computer Records

The systems administrator's responsibilities should include maintaining log records for every computer used in the business, including the make, year, model and serial number as well as the details of the software programs and updates that are installed on each computer.

Keeping a computer log for each computer and regular updating this information can help your company:

- Monitor all software currently used by the company, including registrations, licensing agreements and versions.
- Budget for upgrading equipment and programs.
- Determine if programs are no longer required and should be uninstalled.
- Ensure that all computers have the same versions of communication software, virus scanner, and other tools.
- Create opportunities to discuss requirements with individual employees.

- Help reduce the risks by monitoring computers to ensure unauthorized games or other programs are not installed on company systems.
- Maintain records of software fixes and patches and equipment repairs or upgrades, such as installing more RAM on a computer or replacing a keyboard or mouse.

Software

The installation of unauthorized programs is a particularly serious risk to your operations and systems security as they could corrupt or change data or applications. Unauthorized programs could also be a source of debilitating worms or viruses. If your system is contaminated with malicious software, your operations could be severely damaged. While an employee may think that installing a game program is a minor violation, every violation of the

company's software policy is potentially a major risk to the company's operations.

Make sure all employees understand the importance of following company procedures and approvals for the purchasing, downloading or installing and upgrading of software applications.

The ready availability of many software programs over the Internet makes the downloading of trial versions of products or time-limited versions (called "crippleware") tempting and easy. However, if the software downloaded over the Internet is not properly registered, your company may be in violation of software licenses, a situation that could put your company at risk of penalties and loss of reputation. These risks, along with the risk of malicious viruses, are just as applicable if employees install unauthorized programs that they have brought into the office on a CD-ROM.

Consider penalties for installing software that is not procured through the company's approved procedures.

Protect Your Company's Data and Computer Systems

Make sure every employee is fully aware of the importance of complying with the company's policies and guidelines for using company computers. Appoint a systems administrator who is responsible for maintaining careful records of your computer systems and applications and ensuring compliance with the company's computer policies. Talk to your chartered accountant about these and other measures that can help you protect your company's data and systems. ■

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.