

Business Matters

FEBRUARY 2015

VOLUME 29 | ISSUE 1

TAXATION

Income Tax Fraud

Make sure you hire the right person or company to prepare your income tax return.

According to the Canada Revenue Agency (CRA), 28 million people file income tax returns each year and of that number, 50% use tax preparers. Tax preparers can register with the CRA to use **EFILE** to transmit the completed return through an encryption technology that instantly acknowledges the tax return has been received.

So, what could possibly go wrong for the taxpayer? Unfortunately, not all tax preparers are honest. And, these less-than-honest ones take advantage of the fact that prospective clients believe the tax preparer:

- is an expert and will prepare the return better than they are able to do it themselves
- will find ways to get the maximum refund



- has the taxpayer's best interest at heart
- is registered to **EFILE** tax returns and thus the CRA vouches for their integrity

Fraudulent Income Tax Preparers

Most income tax fraud relies upon the ability of the fraudster to:

- gather information about the taxpayer
- promise a refund for the taxpayer
- convince the taxpayer to have the refund sent to the tax preparer

- convince the taxpayer to pay by cash or debit card
- prevent the taxpayer from understanding how the refund amount was calculated.

Easy Access to Your Information

Information about the taxpayer is easy to obtain. Most taxpayers are asked for their last year's tax return, which contains all the information required for the current filing. The taxpayer may also be asked for their account number, personal identification numbers and answers to security questions to make it easier for the tax preparer to access and manage a personal tax account.

EFiling

Electronic filing has many benefits. On the positive side, it is faster and "paperless." Unfortunately, the negative side means that it is easier for unscrupulous tax preparers to defraud the CRA. As long as the tax return is accepted electronically, the CRA will likely issue a computer-produced refund to the taxpayer. It is only later, after the system has set up audit thresholds and starts requesting information from the taxpayer, that the fraud may be revealed.

Falsified Input

The dishonest tax preparer completes and prints the tax return based on the data provided by the taxpayer. The taxpayer assumes the tax preparer submits this return to the CRA. However, the tax preparer actually submits a different return on which the numbers have been changed to provide a refund, whether the taxpayer is entitled to one or not. Tax preparers have a multitude of ways to create a refund to be deposited into the tax preparer's bank account. The fraudster can claim:

1. higher expenses or lower revenue for sole proprietors who also receive T4 income. A loss from self-employment is applied against the T4 income to produce a reduction of taxable income and thus a refund of T4 income tax remitted by the employer. If the client is also a GST/HST registrant, the tax preparer may be able to obtain a refund in this area as well.
2. a deductible RRSP contribution higher than that made by the taxpayer
3. tuition fees or medical expenses higher than those paid by the taxpayer

4. married or common-law status
5. non-existent dependants
6. excess or non-existent union dues
7. charitable donations the taxpayer never made
8. rental payments or property taxes in excess of the actual amounts.

Where Did the Money Go?

If the CRA refund is deposited into the tax preparer's bank account, the preparer quickly removes it and disappears to parts unknown. If the refund is not deposited to the tax preparer's account, the tax preparer may simply base their fee on a percentage of the falsified refundable amount. The taxpayer, elated by the high refund, gladly pays the exorbitant fee unaware of repercussions from the CRA when the fraud is revealed.

The taxpayer, not the tax preparer, is responsible for the accuracy of the information filed.

Recourse against a Fraudulent Tax Preparer

The taxpayer may mistakenly believe the tax preparer is ultimately responsible for the fraudulent tax return. This is not true. The CRA takes the position that the taxpayer is responsible for the accuracy of the personal tax return. On the signature page, just above the taxpayer's signature line the words: "I certify that the information given on this return and in any documents attached is correct, complete, and fully discloses all my income" provides a reminder of the taxpayer's responsibility.

Certainly, the taxpayer may have recourse against tax preparers who file fraudulent returns. Realistically, however, it may be impossible for the taxpayer to locate the fraudster and even then, the legal cost and time involved to sue may not be worth the expense.

A CRA Audit

Unfortunately for the taxpayer, the CRA may be tardy in requesting information from the taxpayer about reassessed years. Thus, if fraudulent filing has occurred

over more than one tax year, the sudden emergency of having to respond to a reassessment covering several years will come as a shock to the taxpayer.

For the taxpayer the results of a CRA audit will create the following realities:

- Costs will be incurred to review the reassessments and address issues raised by the CRA.
- The new tax preparer will undoubtedly have to process a new tax return using the proper information in order to compare it to the fraudulent submission.
- The taxpayer will have to pay the taxes on the amended amounts and will have to repay the amounts refunded by the CRA based upon the falsified returns.
- Penalties and interest may be assessed.

Check Out the Tax Preparer

The majority of tax preparers are honest, hard-working individuals who strive to provide a service that will meet the requirements of the CRA. But, as in every occupation, there are those who will take advantage of the trust placed in them. In our high-tech world, relying on the Internet or hard copy to validate someone's credentials is problematic. Anyone can design a home page, create or embellish qualifications and print a certificate establishing them as a qualified tax expert. None of the following individual checkpoints guarantees the honesty of the preparer, but collectively they may provide some assurance of the tax preparer's credibility:

- Talk to your friends. They may be among the 50% of individuals who use a tax preparer. Find out how long they have used the service and whether there have been any major reassessments.
- Talk to people in business. Most use the same qualified professional to prepare their corporate and personal tax returns.
- Ask the tax preparer for credentials. CPAs are registered with the various provincial institutes and should be able to provide a licence or membership number. Don't hesitate to contact the various provincial institutes to determine whether an individual is in good standing.
- Your tax preparer should be available year round. You want a firm or individual with a locally

established presence. Online businesses allow data to be processed anywhere in the world. But, as a taxpayer, you should consider whether you want a virtual relationship in the Internet hinterland or a flesh-and-blood relationship with someone in your community with whom you can meet one-on-one to discuss tax issues.

- Ensure that you receive a complete and unabridged copy of your tax return, whether the return is hard copy or PDF.
- Review the tax return for reasonableness before you sign the T183, "Information Return for Electronic Filing of An Individual's Income Tax and Benefit Return" that allows the tax preparer to **EFILE** your return. If you have qualms about the tax return, do not sign and ask for all data to be returned.
- If you are still uneasy about the tax preparer, but your return appears reasonable, request the tax preparer to **EFILE** the return while you wait for confirmation the CRA has received it.
- Never sign an unfinished tax return or a blank T183 or T1013 "Authorizing or Cancelling a Representative."
- Do not provide permission for the funds to be deposited directly into the tax preparer's account. Carefully read Part C of form T183.
- Always obtain a copy of your signed T183 form if you have doubts about the integrity of the tax preparer. The signed form will not prevent the individual from changing the form before transmitting the tax return but it will provide evidence the tax preparer misappropriated your funds.

Consider Using a CPA

Whether you are going to a tax preparer for the first time or switching to another, carefully vet the tax preparer's qualifications. Tax time is stressful enough without the added risk of future problems with the CRA. Establishing a long-term relationship with a trusted tax preparer allows them to understand the changes taking place in your life and determine whether tax treatments are available to minimize the taxes payable while at the same time satisfying the requirements of the CRA.

TECHNOLOGY

Thumbs Up!

USB flash drives are a great business tool – with a few risks to keep in mind.

The thumb-sized (or smaller) USB flash drive is a marvellous development in miniaturization that has revolutionized portable file storage. Fast, small, affordable and convenient, the flash drive has become indispensable. Flash drives have become so ubiquitous, they are frequently handed out as corporate-logo-embossed key fobs loaded with marketing and promotional material that can easily be reviewed by clients.

It all started in the mid 1980s when Toshiba developed the NAND flash memory that morphed into the USB flash drives we use today. The first commercial drives sold in the year 2000 held eight megabytes (MB), but within two years they had reached an astounding 64 MB. Today, a flash drive with storage of one terabyte (TB) is available, if you have the cash — a one-TB flash drive currently costs about \$1,200.

The ability to store endless amounts of data so easily has resulted in the proliferation of USB flash drives (approximately 80 million are sold each year). Along with this extreme convenience and utility, however, comes an unprecedented threat to personal security.

Why Security Is an Issue

- Drives are small and subject to loss or misplacement. Most do not have access codes and thus, once found, can be downloaded by anyone.
- The loss (or theft) of company data such as employee names, addresses, birthdates, social insurance numbers, family-member information and bank information on an unencrypted flash drive could have serious consequences.
- Cyber criminals are starting to write viruses and worms that can penetrate the drives through the USB port. Once the bug is on the drive, the malware eventually finds its way to the host computer. If the computer is connected to a network, the entire system could be compromised.



- Discipline is required to ensure that USB flash drives do not compromise company data.

Best Practices

Most owner-managed businesses will not be a target of cyber-attack. Nevertheless, protocols should be in place to reduce the chance of loss or the compromising of important information that is transferred to USB flash drives at the end of every working day. The following practices will reduce risks:

1. Staff should be provided with corporate USB flash drives. Personal flash drives should never be used on corporate computers.
2. All USB flash drives should be scanned for viruses, even within the same office, before the data is transferred from the flash drive to the host computer.
3. All USB flash drives should have the staff member's name and telephone number written onto them. If that is not possible, ensure the flash drive is attached to a lanyard or key-chain tag with the name of the user. If possible, a telephone number in indelible ink should be written on the tag so it can be returned to the owner if lost.
4. Instill the habit of returning the flash drive to a specific location as soon as data has been transferred; a drive left on your desk — even for a short time — may be accidentally picked up by a co-worker, cleaning staff, dropped into the trash, or placed in a client file.
5. Just as staff should never leave paper with confidential information on their desk at the end of the day, so USB flash drives should also be secured.

6. Employees should know they have a responsibility for security of the flash drives and the data they contain. They must understand the harm that may be done through loss of confidential corporate information.
7. Ensure your IT administrator uses a mandatory scan to parse sensitive data to prevent copying.
8. Use encryption. Encryption programs may be purchased separately or you may use software included with your operating system, such as Windows Bit Locker, to encrypt your files. Encryption software may be configurable to enforce your IT policies. Be sure to research the software before purchase to ensure the software package can accommodate the level of security your company requires.
9. Purchase USB flash drives that have built-in security features such as encryption and authentication (e.g., a password or fingerprint). Advise employees that company-issued flash drives should only be used to store the company's information, and are not for personal use.
10. Do not permit any apps or programs, regardless of how helpful they may appear, to be downloaded from any source until they are reviewed and approved.
11. Never plug in a device with an unknown origin.

Final Words

Even if it is not possible to stop the most malicious of attacks, most owner-operated businesses are probably not likely targets of hackers and malware-encoded USB flash drives. It is more likely that a small- to medium-sized company would be compromised internally by some failure to follow good security practices. For the majority of owner-operated ventures, keeping computers upgraded with the latest security patches, web-filtering and anti-virus software will isolate and quarantine most attacks that result from not following the rules. If you are able to balance your security needs with the ability to conduct your business, then you can embrace the convenience and versatility of the USB flash drive in your day-to-day operations.

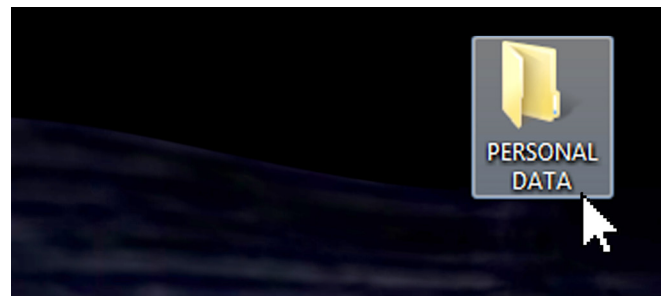
MONEYSAVER In the Event of...

Executors will thank you for your well-organized personal files.

Twenty years ago, the executors of an estate would find most information about the deceased's assets in a valuable-papers file. Hardcopy documents contained the information needed to determine the value of investments, debt, tax requirements, etc. necessary for carrying out the wishes of the deceased and meeting the demands of the Canada Revenue Agency.

Electronic Files Instead of Paper

Electronic documents can now provide evidence of past transactions. These documents are easy to create and store and are accepted as evidence by the courts. The problem for executors, however, lies in how well



transactions were recorded and organized by the deceased. Those who set up a computer-filing system may find the following of benefit.

Getting Started

Create a main folder with an easily identifiable name such as **PERSONAL DATA**.

Within the main folder, set up various subfolder categories such as:

1. banking
 - credit cards
 - line of credit
 - mortgage
 - TFSA
 - RRSP/RRIF
2. investments
3. insurance
 - home
 - vehicle
 - life
4. household expenses
 - electricity
 - water
 - property taxes
 - heat
 - telephone
 - Internet service provider
 - cable television
 - security system
5. offsite server storage
6. personal property
7. income tax, CPP and OAS

This system will permit your executors to understand quickly how the information has been organized.

Organize Email

Set up electronic filing categories and sort each document into the appropriate category. Data received in hard copy should be scanned and saved in the appropriate electronic folder. The original hard copy document should also be saved in a filing cabinet.

Establish annual subfiles within the various categories for data received yearly, quarterly or monthly. Owner-managers should create parallel categories for business documents.

Passwords and Encryption Keys

Establish a protocol for password storage. For example, create a subfolder listing the password for each

account, or store them in a separate password file.

Passwords are needed to log onto the:

1. computer
2. offsite storage locations, hard drives or USB drives
3. email accounts
4. online banking and investment accounts
5. system provider

The account name, number and the Internet access codes for the Internet provider should be readily available should the executors experience a system failure.

If your computer is set to fingerprint-read or iris-scan only, modify the software to accept keyboard passwords as well.

As a precaution against the loss of electronic data, a copy of the passwords should be printed and stored with a trusted individual such as a family member. Because spouses/partners usually travel together, both may die at the same time. It is wise to provide a secondary trusted individual with a sealed copy of the passwords. You may want to provide your lawyer with sealed documents to be opened on your death.

Existing Hardcopy Data

Keep hard copies in a physical file under the same file name as the electronic copy. A PDF format ensures the document is an accurate facsimile of the original. Original hardcopy documents that need to be kept in physical form are birth certificates, citizenship papers, passports, marriage certificates, and property title or deed documents. A scanned electronic file of these documents should also be created in case the original physical document is lost.

Backup Data

Keep backup copies. In catastrophic circumstances, such as a fire or natural disaster, the original source as well as the backup maintained at home may be lost. Consider storing copies of important documents in an offsite backup facility. Most virus protection companies provide adequate backup to accommodate these files either free or for a minimal charge.

Other Considerations

Provide the executors with the:

- combination numbers and/or location of the keys for home safes
- location of keys for the house, vehicles, business, outbuildings, recreational assets, etc.
- names, addresses and contact numbers of investment brokers, lawyers, accountants or tax advisors
- ownership and insurance papers
- safety deposit box location, box number and location of the keys
- location of the original will.

MANAGEMENT Move It

For a retailer, selling off outdated or unwanted stock requires effort and imagination.

Nothing can be worse for a retailer than to purchase stock, display it for sale, and then find no one wants to buy. Not only has the purchase of this inventory cut into the cash flow, but it also takes up floor space that could be better used for merchandise customers actually want. Seeing the same merchandise day after day sends a subliminal message to regular customers that the store has nothing new to sell or that perhaps the store is having financial difficulties and can't afford to restock with new goods. What can the owner do?

Product Placement

Most impulse purchases are made near the checkout counter. To benefit from this moment, place slow-moving items near the checkout with signage advertising them as this week's specials. Ensure sales staff can talk about the benefits of these products. For example, if the item is a silk scarf, the benefits may be current style, quality, elegant-feeling texture, newest colours, etc.

Pricing

Old inventory must be priced to move. Since you probably do not know the elasticity of demand for every class of product, you should initially set prices as close to break-even as possible with the hope of avoiding a loss.

Good Files Facilitate Settlement

Keeping your affairs in order makes settling your estate easier. Keeping well-organized electronic files is one of the ways to assist your executors settle your estate correctly and expeditiously. Precisely labelled files, readily available and up-to-date passwords, plus asset lists and hard copies of important documents in easy-to-find locations as well as the names and addresses of your lawyer, accountant and other important persons will not only make your day-to-day life easier but will also ensure your executors are able to deal with your estate.



Bundle

If you are having trouble selling a particular product, you might be able to move it by bundling it with a complementary or related product. Bundling enables the consumer to see how the products can be used together. A customer may not buy a router by itself but, if the router is bundled with bits, the package becomes more desirable.

Relocate In-Store Products

If sunglasses are hidden in the corner, moving them closer to the suntan lotion or the swimwear might create sales.

Attractive window displays bring customers through the door.

Displays

Attractive window displays will entice even those who are not at the moment interested in purchasing. Change your displays regularly and place an attractive assortment of products inside the front door. This demonstrates the range of quality merchandise and will draw customers further into the store.

First Impressions

Place slow-moving items near the entrance, and keep the display attractive to avoid giving the impression of a clearance rack. Potential buyers will be enticed by the appeal of low prices before making any other purchase decisions.

Product Knowledge

Sales personnel with product knowledge create sales. When a consumer asks questions about a product, they expect a well-informed answer. Anyone can read a label, but often a consumer will want to know additional information. Encourage staff to become knowledgeable about *all* products, including the ones priced to move quickly.

Discounting Guidelines

Management can offer bonuses for moving items stalled on the floor. However, customers may resist spending if they feel pressure by overeager sales personnel. The commission percentage has to be

structured to prevent erosion of the profit margin. Rather than paying commissions, you can provide guidelines for staff to negotiate a price if they see a sales opportunity. Permitting staff to offer a certain percentage discount will often encourage the purchase.

Websites, Email and Social Media

Perhaps the product is not moving because customers do not know it exists. Keep current and future customers informed with a business website, or by using email, Facebook and Twitter. The website should provide all necessary information about your product line and today's deals. Also, consider investing in photos of merchandise and printable e-coupons that provide discounts on slow-moving merchandise.

Marketing vs. Selling

Every retailer must understand the difference between marketing and selling. Marketing is your strategy for bringing your product to the attention of the customer most likely to buy it. Selling, on the other hand, is the ability to persuade that customer to purchase the product or service that meets their needs. The interactivity between you and your customers facilitated by the Internet should enable you to keep closer tabs on what your customers want and leave you with fewer items lingering on your shelves and needing an imaginative effort to get them out the door.

Disclaimer:

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 Chartered Professional Accountants of Canada for the clients of its members. Richard Fulcher, CPA, CA - Author; Patricia Adamson, M.A., M.I.St. - CPA Canada Editor.

Contact us: patricia@adamsonwriters.ca