

## Uniforms key to knowing who belongs

Since the deadly terrorist attacks of 9/11, companies have begun to adopt employee uniform programs not just for their noted branding and image attributes, but as a means to increase overall security and guard against threats by outside intruders.

By adopting a unified look—particularly one that has been personalized through the use of specific colors and personalized logos—companies have found they can more easily identify who belongs or does not belong within a particular work setting.

Identifying who does or does not belong within company facilities may seem like a relatively routine task, but it can be particularly daunting for companies that have large numbers of staff or visitors arriving or departing on a regular basis, or for organizations with high employee turnover.

Statistics issued by the Uniform and Textile Service Association (UTSA) underscore the attractiveness of uniform programs. The UTSA says approximately 1.2 million employees in North America began wearing uniforms to work for the first time last year, bringing their total numbers to 33 million.

Beyond security, safety can also be an issue that uniforms can address.

Consider food processors and computer chip manufacturers who must continually guard against cross-contamination threats to their products: Within such industries, managers can quickly identify

who does or does not belong in a particular production setting by having their employees outfitted in uniforms color-coded specifically for certain job tasks. For example, a food or electronic chip handler might wear white uniforms while those in packing and shipping could wear red or green. All basic personalization elements would remain the same for branding, but the colour-coding would help to reinforce product security.

Any company launching or reevaluating an employee uniform program for overall image and security purposes should take into consideration the following three measures:

1. Adopt uniforms that would be difficult for others to copy. Uniforms should make use of certain colors and incorporate logos and other unique personalization elements, such as slogans and job titles.
2. Store all uniforms in a secure location for laundering or repairs.
3. Collect uniforms from employees who leave the company.

While security is a key concern

with many companies, so is budget—particularly in today's uncertain economies. However, these concerns are not mutually exclusive since uniform providers develop programs through rental, lease and purchase options.

A rental program, which is turnkey in nature—from delivery, to cleaning, to repairing and replacements—works best for companies that prefer to make no up-front investments and are interested in having a service provider assume overall responsibility for their program's management.

A leasing program offers a lower cost structure but employees are responsible for laundering their own work garments. This means an employer must police the cleanliness of all employee uniforms. With the straight uniform purchasing option, a company makes a single, up-front investment and must manage its entire program.

No matter what option is used to obtain uniforms, a personalized employee uniform program can place a significant hurdle in the path of an unwanted intruder.

*Chris Harnett is a branch manager with UniFirst Corporation, a uniform and facility services provider in Pickering, Ontario. He may be contacted directly by calling 905-426-6271 or by e-mailing Christopher\_Harnett@unifirst.com. www.unifirst.ca.*



Chris Harnett,  
UniFirst Corporation



Different colour patterns or combinations can signal specific employee job functions within companies and, in turn, improve security to guard against outside intruders.

## Enhance YOUR Business Image

Providing Industrial Garments to Corporate Casual Attire since 1936, UniFirst offers the right uniform options to meet the needs of your business. We also offer various Facility Services like Floor Mat and Restroom Products to be your one-stop, value-based service provider. So call our Pickering Office for a FREE, no obligation service evaluation:

905.391.9044

unifirst.ca

**UniFirst U1st**  
Uniforms • Services • Solutions



# The Bulletin...by mail

Information from the Ajax-Pickering Board of Trade

## Winter Edition, 2008

As we get set to celebrate the holiday season here at the Ajax-Pickering Board of Trade, we considered what we hope is a busy retail season for our members and wondered if everyone is prepared for the rise in consumer fraud that is the inevitable side effect of the crush of Christmas shoppers.

Inspired by the Board's Nov. 26 'Fraudulent Event', we turned to the experts on fraud and the broader issue of safe business practices for our Winter Edition of the *Bulletin... by Mail*.

As important as it is to be vigilant against credit card fraud and counterfeit cash, we also considered the importance of securing data in your computer systems, protecting your business and staff on site against unwanted visitors, as well as the insidious problem of identity theft.

Enjoy this edition of the *Bulletin... by Mail* and take note of some of the excellent suggestions offered in the following columns to help you thrive in the face of common threats to business success.

### PRINTING GENEROUSLY PROVIDED BY:



905.428.3981  
accurateimaging.ca

## No lock strong enough to stop ID thieves

The next time you take a walk through your neighbourhood note all of the window stickers and lawn signs warning potential thieves that the occupants have a high-tech security alarm system ready to sound off the minute the doors or windows are jimmied.

Thieves today do not have to strain a muscle or break a sweat to steal from you. Stealing your electronics, jewellery or cash is too risky and the rewards too small in comparison to stealing your identity and selling it over and over and over again.

Identity theft is the fastest growing crime in the world today and it can be happening to you while you go about your life feeling safe and snug in your secure home. From the moment we are born until we pass on, valuable information is collected and stored in data bases on each and everyone of us. Today's computer age thief can assume your full identity in just minutes, but it could take you months or even years

to realize that someone is using your good name for their personal gain.

There are five common areas of identity theft. We mostly hear about financial/credit fraud which includes our bank accounts, credit cards and mortgage fraud. But this is just 25 per cent of the problem. Our Social Insurance number, health card, driver's licence and our good character are of more value.

With these pieces of the puzzle someone can basically become you and live the high life until they destroy your credit and good name. Then they move on leaving you holding the bag for the mess they have made of your life. I want you to know that no one will love you more, appreciate you more, or adore you more than your very own identity theft criminal. ...please see 'You' on page 2



Shirley Bankey,  
PPL Legal Care  
of Canada

## Backup: Is yours a disaster waiting to happen?

**In today's business environment, your business runs on its data – you collect it for Sales and Marketing, Accounts Payable and Receivable. Your e-mail is often the most used application you have. So how critical is this for your business? If you lost all you data today, how would it affect your business?**

Studies continue to show that more than 80 per cent of businesses don't backup properly. This, in spite of evidence that shows us that among companies that lose their data in a disaster, 50 per cent never reopen and 90 per cent are out of business within two years.

Even those that think they have a sound backup strategy find themselves in trouble when they go to restore a file.

### Practical Steps to Improve Your Backup:

1. For a small business with only a few PCs, store all your critical data on one PC.
2. Take time to understand what is being backed up and what to restore.
3. Organize your data. Separate older data that is no longer used and archive

separately. This will make your daily backups smaller and easier to manage.

4. Check backup logs often. If there are errors, find out why and fix it.
5. Store the backup in a fireproof safe with one set stored off-site (NOT the trunk of your car).
6. Backup and store off-site the original disks from the software you run. This step alone will save you time and frustration.
7. Online backup services are a powerful way to add another layer of protection. It is an automated way of storing your critical data offsite. If you use an online backup service, don't considerate it as your only backup (that "all your eggs in one basket" thing).
8. In case of a disaster, document who to call and what programs/data to reinstall first. This will get you running quicker during a disaster.
9. Ensure your e-mail files are being backed up. This can be tricky; the data is often buried deep in System Folders.
10. Export your Contacts and Calendar information to your centralized folder on a regular basis.
11. Archive old e-mails and attachments. Archiving moves the e-mails to another file and reduces the size of your main e-mail file – making it easier to backup.
12. If you find this all confusing and

scary - bring in help. It will be the best investment that you make.

Unfortunately, we sometimes don't find out we're unprepared until it's too late.

If you're concerned about your backup and your ability to recover, get help. Don't wait until you have lost data and can't recover it. In the long run, it may turn out to be the best investment that you have made. But just don't turn over this issue to someone else, talk to him or her. Find out what they are doing and how well you are protected. Understand what your responsibilities are and what help they will bring if you ever need it. Understand what is protected and what isn't. Financial and technological constraints do not allow for every piece of data on every computer to always be backed up and available for immediate restore. Prioritize what needs to be restored.

In the end, your data is your business and you are responsible for it.

*Rob Fraser is the president of ClubIT, a company offering data protection and IT services for a wide range of businesses.*



Rob Fraser,  
President of ClubIT

## Protect you business against fraud by being aware

BY MARTIN FRANSSSEN

### When you think of fraud what do you think of?

"It is just white collar crime."

"Nobody gets hurt. It is a victimless crime."

"Oh, the banks can afford it. After all, look at those record-breaking profits."

"It hasn't happened to me, so it doesn't affect me."

I am sure if you were to ask the 27,000 Canadians whose debit cards were compromised in 2003, to the tune of \$44 million, you would get a much different response.

### According to the Retail Council of Canada:

- credit card losses in 2005 due to fraud were \$201 million
- debit card fraud losses were \$70.4 million (a sharp increase from 2003)
- 422,447 passed and seized counterfeit currency

If you were one of the 27,000 in 2003 then it did happen to you. If you were a shopper in 2005 then it happened to you. If you had a credit card in 2005 it happened to you. Unfortunately it is happening daily on an ever-increasing basis.

We need to increase awareness of fraud in hopes that knowledge will lead to prevention. With the advent of technology and our dependence on it, new and lucrative avenues for fraud are now available.

### So how do I protect my business?

Awareness, education and continued vigilance is your best defence. As technology is used more and more in our everyday busy lives at home and at work we become more and more susceptible to becoming a fraud

victim. As the courts tend to look at fraud as a victimless crime, the penalties imposed are routinely light.

And even with a successful prosecution, the courts are leery of imposing a restitution order knowing that doing so will often just cause the continuance of more criminal activity. Therefore, at the end of the day, we are left with limited satisfaction and a whole lot of frustration.

### Ways to protect you business/workplace include:

1. Consider requesting a Criminal Information Request (CIR) for your employees. Although this is not a fail-safe protection, it is another means

### Frauds Aimed at Businesses:

1. Business cloning
2. Spoofing e-commerce website
3. False accounting
4. Asset misappropriation
5. Insurance fraud
6. Computer fraud
7. Invoicing fraud – Charged for product or services never received

available to assist in the employee screening process. The cost (presently \$30 with the DRPS) is minimal compared to your potential losses.

2. Request a second form of photo ID when a customer presents a credit card. Although your

customer may not appreciate this request at first, an explanation that your company is striving to help protect the customer often eases the situation. And if it becomes a standard practice with your business your customers will become accustomed.

3. Check your Interac/credit card terminal daily. Look for signs of tampering.

4. Complete an independent accounting audit and inventory at least every two years.

5. Limit the amount of information you collect from your customers and safeguard it.

6. Refer to the various business organizations and associations, such as the Ajax-Pickering Board of Trade,



websites, etc. and become aware of the latest fraud activities and methods. Take this knowledge and assist your front line staff in their awareness and methods of prevention.

### One man's trash is another's gold

One of the best ways to protect yourself and your business is to ensure that no document, including junk mail, transaction receipts, magazine subscription labels, bank records, customer lists, etc. never appear in the garbage. Buy a shredder or use a bonded shredding company.

Fraudulent activity is not new and continues to increase annually. We are all vulnerable to it and, although in the eyes of the courts it may be a victimless crime, just ask someone who had their wallet and identity stolen if they were a victim. In reality our judicial system is not equipped to handle the ever-increasing case load. We all must take steps to protect our name and our business.

The old adage "An ounce of prevention is worth a pound of cure" is completely applicable when protecting against fraud.

*Martin Franssen is a Criminal Investigations Fraud Investigator for the DRPS.*

## You don't have to be wealthy to be a target

...continued from page 1

They love you for your great credit rating. They appreciate your clean driving record. They adore you for not owing any back taxes.

You don't have to be wealthy to become a victim. Imagine having collection agencies harassing you for money you never borrowed, Revenue Canada wanting back taxes for a business venture you never had, having your car insurance cancelled for speeding tickets you never received or drunk driving charges in your name.

The worst case scenario would be the life-threatening possibility of numerous people using your medical card and having their medical histories

mixed in with your medical history.

You are now in a Legal Nightmare. Would you know what to do if it happened to you? Would you have enough money for a lawyer? Would you have the knowledge and available time during business hours to clear up credit reports, fill out and submit affidavits, deal with lawyers and make the endless telephone calls required to solve the problem and restore your credibility?

This sounds overwhelming and costly, doesn't it? You need more than "do it yourself" information if this happens to you. PPL Legal Care of Canada is a company that is meeting this need head on with its Identity Theft Shield, a product that has helped thousands of identity theft victims with the difficult task of reclaiming and restoring their

names and their credit.

Identity restoration means that licensed investigators will work to correct damages caused by identity theft. This includes working with affected public agencies, like the credit card companies, financial institutions, credit repositories, Phonebusters, Passport Canada, and law enforcement personal.

In addition, fraud alerts will be sent on your behalf to all three credit bureaus and affected companies and agencies.

This column has only scratched the surface of this devastating crime.

**Shirley Bankey** is an Independent Associate for PPL Legal Care of Canada. For more information, e-mail her at shirley@ppl-legal.ca

To advertise in our next The Bulletin by Mail, contact the Board office at 905.686.0883 or e-mail info@apboardoftrade.com

**KNIGHTS ON GUARD**  
To Secure, Deter & Protect

Private Investigations		Parking enforcement
Retail Loss Prevention		Security Officer Service
Labour Disputes		Alarm Response
K-9 Services		Mobile Security
Man-Down Team		Office / Factory / Warehouse
CCTV & Alarms		Condos / Apartments
Off-Site Video Monitoring		Construction Yards

**Bill Dimkovski & Steve Dimkovski**  
905-427-7863 • 1-866-427-7863

1048 Toy Ave. - Suite 101 Pickering, ON L1W 3P1 Tel: 905-427-7863 1-866-427-7863 Fax: 905-420-9957	121 George St. N. - 2nd Floor Peterborough, ON K9J 7Y8 Tel: 705-742-8699 1-866-427-7863 Fax: 705-742-9747	Niagara Square Shopping Centre Security Office 7555 Montrose Rd Niagara Falls, ON L2H 2E9
--	---	--

www.KnightsOnGuard.com