

# FORENSIC ACCOUNTING & FRAUD



## Internet, e-commerce opens electronic avenues for fraudsters

By Peter Fatijewski  
and Kevin Melnichuk  
Grant Thornton  
Toronto

Imagine one of your larger corporate clients is sitting at his desk. His administrative assistant walks into the office and appears to be concerned. She informs you that the police have called.

Unbeknownst to your client, the police have found his corporation has taken out significant loans that appear to be financing terrorist activities half way around the globe.

Could this really happen to your client? Absolutely! Your client could become the victim of corporate identity theft and it's the type of crime that's much easier to commit than you would think possible.

It's important that you ask the right questions at the right times to protect your client against being a victim of crime. Based on the level of risk involved, it is necessary that proper controls are set up to safeguard sensitive corporate information.

In addition, employee screening should be carried out prior to the start of employment and periodic screenings of current employees with access to confidential corporate information.

When you work on an engagement such as an incorporation, merger or acquisition, a real estate transaction or other types of financial transactions, you can help the client understand the threat of identity theft and offer some solutions. Does your client really know who he is dealing with?

This is a real threat and a simple example can illustrate the point.

An actual police case involved two individuals who were arrested in connection with corporate identity theft. These individuals targeted leasing companies that leased computers to major corporations.

In total, they were able to fraudulently obtain \$150,000 US. To perpetrate this crime, these individuals created false credit applications in the names of some large, well-known high-tech companies.

The leasing companies felt the applications were legitimate and called the telephone number provided on the application. The telephone number was not the leasing companies, but was linked with the individuals who were committing the crime.

If the leasing companies had simply looked up the corporate contact information either through the telephone book or the Internet, it would have been apparent that the telephone numbers listed in the credit application were incorrect and the fraud scheme may have been avoided.

This fraud scheme highlights the amount of information that is avail-

able through the Internet. All the information necessary to create a false credit application (*i.e.* corporate officials names and positions, corporate logos, *etc.*) was easily accessible through the Net and the fraud was quite easily perpetrated as a result.

We have all heard about personal identity theft and how devastating it can be as a victim. But can identity theft leave corporations vulnerable? Definitely! You may wonder how.

Cheque fraud, threat from your employees, e-commerce and the Internet all leave your corporation exposed and vulnerable. Some writers even go as far as referring to corporate identity theft as a form of "economic terrorism."

Corporate identity theft may include such things as cheque fraud, employee theft of corporate information, theft of letterhead, theft of client lists, e-commerce and Internet risks.

### Cheque Fraud

Cheque fraud has been and still is a major risk for corporations. With the advent of technology, identity theft and cheque fraud has become easier. Laser printers, scanners and digital cameras can all be used to produce counterfeit or altered cheques.

Through several investigations into cheque frauds, it was noted that proper protocols do not exist surrounding the safety, storage and issuance of cheques and signature stamps. Cheques can be misappropriated in a variety of ways — from the mail, by employees in the workplace, from couriers, or even from the printers that print the cheques.

Once the cheques have been stolen, they are either counterfeited or altered. These "fraudulent" cheques, which can range from sophisticated copies to poor quality copies, are easily being negotiated and cashed at financial institutions by unsuspecting bank employees or through ATM's by direct deposits.

Both methods are effective, as it is clear that there is a lack of training to distinguish between a legitimate and fraudulent cheque. Unfortunately, security features and/or controls put into place have not deterred the risk of cheque fraud.

### Employee Risk

Various studies show that the greatest risk to a corporation comes internally from its employees. Employees having access to confidential corporate information, banking records, financial information and other business information may be targeted by criminals to buy or extort that information from them. An employee who has the propensity to commit fraud can profit from the theft of this information.

One specific risk area is a corporation's customer information. Customer information such as credit cards, banking and other data can be sold to criminals, your competition or could even be used personally by the employee.

A simple letterhead can be used to create a false trading history, letters of recommendations, and ultimately to set up false bank accounts and apply for loans. RCMP and immigration officers uncovered a scheme whereby stolen letterhead was used for the purposes of providing false sponsorship letters to obtain Canadian visas.

Can you imagine what a criminal could do with company credit cards or banking information?

### E-commerce

With e-commerce becoming more and more prevalent in business, some feel that identity theft online will become the leading source of identity theft, replacing credit card fraud.

The Internet has allowed for much greater access to company information such as logos, trademarks, Web sites, names and titles

of key employees, and in some cases, even copies of the signatures of these key employees.

In the latest scam, referred to as "phishing," fraudsters seek out companies' customers' financial information through the use of e-mails, which direct them to a "look-a-like" Web site.

With limited skill, anyone can set up mirror Web sites and easily obtain the information they want. Given the enormous technical resources they have on hand, organized crime has become more and more involved in identity theft in all of its various forms.

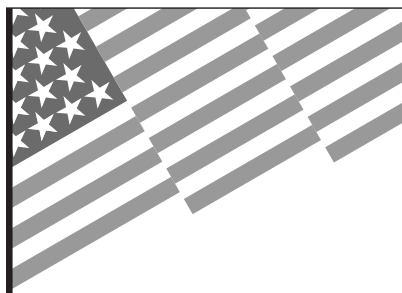
There were instances of bank customers that received e-mails appearing to be from their bank, but in reality were from organized crime groups, redirecting them to a replica site so that they would be able to obtain customers' names, accounts numbers and passwords.

Though we are just scratching the surface, identity theft should be of great concern for businesses. Identity theft is no longer a crime committed by the average criminal — evidence has been uncovered in numerous cases that link it to orga-



nized crime and terrorist groups, such as those responsible for the September 11, attacks on the United States.

*Peter Fatijewski is a practice leader in investigations and Kevin Melnichuk is a forensic accountant with the Forensic Accounting and Investigative Services (FAIS) team at Grant Thornton LLP, an accounting and management firm. They can be reached at pfatijewski@grant-thornton.ca; kmelnichuk@grant-thornton.ca, respectively.*



## U.S. TAX CHANGES

Get Updated Now!



### U.S. Books Published Recently

#### Forensic and Investigative Accounting

From fundamental concepts to real-world case studies.  
August 2003 ..... Can\$164

#### 2004 Miller International Accounting/Financial Reporting Standards Guide

Oct 2003 ..... Can\$195

#### Miller GAAP Guide 2004

Oct 2003 ..... Can\$182

#### U.S. Master Tax Guide 2004

Nov 2003 ..... Can\$76

#### California Tax Guide 2004

Florida Tax Guide 2004

Illinois Tax Guide 2004

Mass. Tax Guide 2004

Michigan Tax Guide 2004

New Jersey Tax Guide 2004

New York Tax Guide 2004

Ohio Tax Guide 2004

Penn. Tax Guide 2004

Washington Tax Guide 2004

Dec 2003/Jan 2004 ..... Can\$76 each

#### Internal Revenue Code

Dec 2003 ..... Can\$112

#### Practical Guide to U.S. Taxation of International Transaction (4<sup>th</sup> ed.)

Nov 2003 ..... Can\$144

To order: 1 800 268 4522

#### To receive your CCH U.S. books catalogue:

Contact your local CCH Account Manager at 1 800 461 5308 or Benoit Filion at bfilion@cch.ca