

An interview with David Harris, Canada's "Dental Fraud Guru"

by bridge editor, Susan Boyd

the bridge (tb): Tell us a bit about yourself.

David Harris (DH): I am the President of prosperident, a company I started in 1989. This is the only organization in Canada specializing in fraud prevention, investigation and forensics for dentists. Before prosperident, I worked in a number of jobs, including doing investigations and some military service (where in one interesting stint, my job was to break into secure military installations – this gave me an amazing insight into how criminals think). Along the way I received degrees in applied mathematics and business and professional designations in accounting and banking.

I got involved with dealing with dental fraud almost by accident – a dentist friend was defrauded and, knowing my background, asked for help. Bill Hiltz, a specialist in data mining and dental informatics, later joined as Chief Fraud Examiner and provided the missing piece.

tb: I think the question on the minds of most dentists is "How likely am I to be a victim?"

DH: There are two credible studies, which provide similar results. The American Dental Association's November 2005 Community Brief suggests a fraud rate of 52% and a 2007 Dumolin and Associates survey found that approximately 60% of surveyed dentists had been victimized. Both studies are American; statistics specific to Canada are not available. However, we do work in both Canada and the U.S. and don't see systemic differences in fraud prevalence.

tb: This seems high compared with similar businesses. Why?

DH: The conventional answer is that dentists are poor businesspeople. I don't accept this "blame the dentist" hypothesis – I think causes are environmental, and I often point to three specific factors – lack of independent monitoring, outdated control systems, and barriers to information access.

One of the most basic controls most businesses have is customers comparing their purchases with invoices and refusing to pay for discrepancies. However, in many dental transactions, the "customer" is an insurance company that is not present at treatment, and the patient doesn't have sufficient knowledge of dental treatments and procedure codes to verify treatment. This lack of independent monitoring is a weakness that is frequently exploited to steal from dentists.

Control systems used in dental offices have changed little in the past half-century. However, fifty years ago, most dental offices were managed by the spouse of the dentist. This is no longer the case. Over the same period, the complexity of the flow of funds in a dental office has increased dramatically (debit/credit cards, internet banking, etc). Control systems simply haven't adapted properly to reflect the current reality.

The third factor is computerization; many dentists have a relatively low knowledge of their dental software and are totally dependent on staff to produce information used for monitoring. Many dentists aren't sure what to ask for and larcenous staff may "filter" information given to the dentist.

tb: How much money is typically stolen?

DH: It varies widely. In 2008, the average theft we documented was \$109,000; however this is understated because investigations often stop once we have documented sufficient theft to make maximum claims under employee dishonesty coverage and to prosecute. My gut feeling is that the average theft is about \$180,000. Of course, the true cost to a dentist/victim is far more than what is stolen when remediation costs and the dentist's lost time are considered. We recently investigated a fraud where we stopped counting at \$609,000 – the true number was much higher.

tb: Are some dentists more likely to be victimized than others?

DH: Many dentists believe that certain practices are “safe” from fraud. For example, rural practitioners often think that fraud only happens in cities; many specialists think that fraud is a problem for general dentists.

In reality, fraud is caused by a confluence of three factors. These can combine in any practice, and when they do, fraud is inevitable. We have found some of the biggest frauds in practices most dentists would consider “safe”. I think the unwarranted perception of safety (and a corresponding lack of scepticism) contributed to the magnitude of these thefts.

tb: So what are these factors?

DH: First, there must be a larcenous employee. I characterize employee/thieves as “dishonest” or “desperate”. Dishonest employees are career criminals who happen to target dentists. Proper hiring practices can keep these people out of your office.

“Desperate” employees have been honest, loyal employees for years when some type of financial catastrophe occurs that, in their eyes, leaves them with few alternatives. Once a desperate employee has exhausted their other options, they begin stealing from the dentist.

The second factor is that the office gives the employee the “Three A’s” – Access, Authority and Ability to Conceal the thefts. Finally, the detection systems used in the office are inadequate to bring the fraud to the dentist’s attention.

Thefts by “desperate” employees typically continue until detection. Amounts stolen can be staggering.

One factor frustrating detection is that fraudulent behaviour mimics that of ideal employees –working long hours (fraudsters need time alone to steal) and they need to control information flow in the office (which makes them look incredibly efficient).

tb: So what can a dentist do to prevent fraud in his or her office?

DH: Fraud prevention comes in two levels – “do-it-yourself” and advanced. There are many things that a dentist can do – we use the acronym CSI for “Control, Scepticism and Involvement”. Control includes making use of the authority levels present in nearly all dental software, insisting on daily bank deposits, and properly securing “point of sale” terminals.

Scepticism means responding to danger signals and investigating discrepancies. Involvement means things like reviewing reports, handling write-offs properly, and reviewing your software’s audit log. For more advanced protection, we offer a series of advanced controls called fraud-GUARD that makes a practice incredibly resistant to fraud.

We are dissatisfied with how the current generation of dental office software counters fraud. We are working with a couple of software companies on developing a fraud-resistant software version – availability should be within the next year.

tb: What should a dentist do if he or she suspects fraud?

DH: The short answer is that they need immediate professional help. Our approach is to conduct a silent “probe” that will allow us to determine whether there is fraud. This probe is done by us remotely, without the employees ever knowing it was conducted. If fraud is confirmed, the dentist can move pre-emptively to prevent further theft and protect evidence. If fraud is not occurring, the dentist would rather have staff unaware that their integrity was questioned.

If fraud is taking place, we will guide the dentist through the process of lockdown and recovery.

tb: What are the professional obligations of a dentist who is defrauded by staff to contact affected insurance companies?

DH: That’s a good question, and I don’t have a simple answer. The insurance companies are of the belief that dentists are obligated to notify them; however at least one provincial Registrar holds the contrary view. Decisions in this area are typically made on the basis of legal advice.

In order to reduce risk to practitioners, we have developed a “whistleblower” program with several insurance companies where dentists who are innocent bystanders of a fraud against the insurance companies may come forward without adverse consequences.

tb: Tell me about the best and worst parts of your job.

DH: There is no denying that I feel a rush of excitement when we find a fraud, especially one that is particularly clever. I also love speaking engagements.

The worst part is dealing with emotionally distraught dentists who have given their trust only to have it abused. Seeing how devastating fraud is to dentists has been the impetus for developing methodologies for prevention and early detection of fraud.

tb: How does a dentist contact you if fraud is suspected?

DH: The best way is to send email to fraud@prosperident.com. This is a priority email address used for dealing with potential fraud. The dentist should provide us with a private email address and a verifiable (i.e. listed in a public directory) telephone number where we may contact them. ■

David Harris is the President of prosperident. For more information on dental fraud, visit the members’ only section of BCDA’s website at www.bcdental.org