

ID thieves try to steal your life and business, too



By Jim Stafford: The Oklahoman

David Petermann insisted he wasn't trying to scare anyone in an "awareness" presentation on identity theft Tuesday at the South Oklahoma City Chamber of Commerce.

Then he looked at the audience and said, "What you really need to understand is that they have your numbers. You are the prime target, and what they are looking for is to steal your life."

Now he had the collective attention of the 22 people attending a seminar presented by Petermann, a certified identity theft risk management specialist from Stillwater.

Just who are "they?"

Well, as Petermann explained it, "they" are not only the thieves who steal your identity but also federal and state authorities designated to enforce a plethora of laws meant to keep data secure and punish businesses that don't meet that obligation.

Oh, and lawyers.

"The next big wave of class-action lawsuits is going to be from data breaches," Petermann said.

"It's going to put businesses out of business, and they don't even know the laws exist," he said.

The existence of massive databases makes everyone vulnerable to identity theft, Petermann said.

The most outrageous example is the personal records of 26 million Americans lost when a laptop was stolen from an employee at the U.S. Department of Veterans Affairs.

Or maybe it was the 45.6 million credit card records pilfered by hackers who broke into the computers of retailer TJ Maxx.

Both are examples of what Petermann called the five common types of ID theft.

Financial theft may be the most well known, but thieves also steal — and use — Social Security numbers, medical identification, driver's license numbers and an area known as "character/criminal."

"Somebody can steal your ID and create havoc in your life, and it's not just financial," Petermann said. "They are not after your money or equipment or your inventory. A new breed of criminals wants your personal information."

Laws that have recently come into play include a pair with ominous acronyms — the Fair and Accurate Credit Transactions Act, or F.A.C.T.A., and the better known Health Insurance Portability and Accountability Act, or HIPAA. Another, the Gramm-Leach-Bliley, better known as the Safeguard Rule, applies to financial institutions.

The far-reaching laws place a lot of responsibility on employers to protect records — electronic or otherwise.

Petermann urged the business leaders attending the seminar to do their homework, assess their vulnerability and take steps to bring their companies into compliance to laws of which they may not yet be aware.

"(Regulators) want to see that you have taken good-faith efforts to establish and have your compliance officers, your written protocols, you've done the mandatory awareness (training) with your employees, that kind of thing," said Petermann, who provides an ID theft consulting service for businesses.

Afterward, Blaine Moore, who operates the South Oklahoma City Sylvan Learning Center, said the strict standards to which employers were being held caught him by surprise.

"I had no idea," Moore said. "I understand they passed these laws to protect us, but at the same time they should have to let us know what responsibilities we have to take to meet the laws. That isn't fair."

As the audience filed out of the room, Petermann reminded them that he was there only to make them "aware" of the threats to their businesses.

Very aware, it would seem.