

The Philadelphia Inquirer

THURSDAY, DECEMBER 13, 2007

Business

WWW.PHILLY.COM

Data Thieves Close to Home

Expert calls friends and acquaintances the biggest source of identity theft.

By Chris Mondics
INQUIRER STAFF WRITER

Greg Parks has his own take, born of years wrestling with data-security issues, on the "Bonnie and Clyde" case now playing to rapt audiences around the globe.

Parks is a lawyer with the Philadelphia firm of Morgan, Lewis & Bockius L.L.P. who advises retailers on ways to avoid lawsuits and even government penalties if their databases are breached and customer information is divulged.

Parks said plenty of media and government attention has been focused on preventing disclosure of customer information from commercial databases. But he said the biggest problem by far was friends and acquaintances stealing from people close to them, the alleged modus operandi of Jocelyn Kirsch and her boyfriend, Edward Kyle Anderton, who have been dubbed a digital-age "Bonnie and Clyde."

"This is a classic case of identity theft," said Parks, one of the lead lawyers in Morgan Lewis' retail-practice group. "The common perception is that computer hackers are able to access your information, or that it is obtained by Dumpster divers. But really, in the vast majority of cases, it involves someone known to the victim."

Yet, because of the potential for mass havoc, lawmakers and regulators are focused mostly on commercial-data leaks.

There are now 38 states with laws establishing varying responsibilities for credit card

companies, retailers, and others when sensitive information gets out. Some require that companies promptly notify customers. Others, including Pennsylvania and New Jersey, give businesses a pass if the information is sufficiently encrypted to prevent access. New Jersey also requires that businesses check with the state police before notifying customers to ensure that ongoing investigations are not compromised.

Congress, meantime, is grappling with legislation that would establish national standards on breaches.

Parks said the problem for retailers was that the issues were so complex, and adjustments in the law so nuanced, that new laws sometimes slipped below the radar and went unnoticed.

That was the case last December with the final phase-in of a federal law requiring retailers to blank out expiration dates and all but four digits of credit card numbers on sales receipts. For years, many retailers had been blanking out credit card numbers on their own, but were unaware that they were legally required to also excise expiration dates.

The law took effect Dec. 4, 2006, and, within days, retailers across the country were hit with class-action suits alleging that they had exposed customers to identity theft by printing the expiration dates on sales slips.

Parks, who is defending a dozen companies against such suits, said there was no evidence that anyone ever had credit card information stolen



MICHAEL BRYANT / Inquirer Staff Photographer

Greg Parks explains to retailers how important it is to safeguard their customer database. On screen, part of his presentation. He is a lawyer with the Philadelphia firm of Morgan, Lewis & Bockius L.L.P.

as a result of the retailers' lapses, or that they represented a real risk.

There is, of course, considerable debate on that point. Michael Donovan, a Philadelphia plaintiffs' lawyer whose firm, Donovan Searles L.L.C., has filed several actions alleging that retailers had breached the law, said that, in the right hands, expiration dates in combination with several credit card digits could be used to access confidential information.

There is no dispute that the proliferation of databases and the evolving law has created new legal exposure for businesses.

To bring clients up to speed, Morgan Lewis held a two-day conference in Dallas last month for retailers, including Radio-Shack Corp. and Bed Bath & Beyond Inc., where the focus was on how to avoid being sued in cases where data are compromised.

The issue is tricky because standards vary from one state to another. California has what generally are acknowledged as the toughest rules. Other states

give retailers some leeway if it can be shown there was little likelihood data were compromised. An example, Parks said, might be the theft of a company laptop containing sensitive information that the thief made no effort to access.

"It becomes a question of doing an investigation," Parks said. "Figuring out what information was on there, and determining whether legally you have to make a notification."

Parks, 36, often advises clients to inform customers, even if there is no legal requirement. But erring on the side of caution can be sensitive, too, because, Parks said, alerting customers when there is no real risk that information was compromised would create unnecessary alarm.

Parks focuses on data security as part of the firm's retail-practice group, which comprises about 30 lawyers and whose clients include Wal-Mart Store Inc., Pep Boys - Manny, Moe & Jack, Rite Aid Corp. and others.

Contact staff writer Chris Mondics at 215-854-5957 or cmondics@phillynews.com.