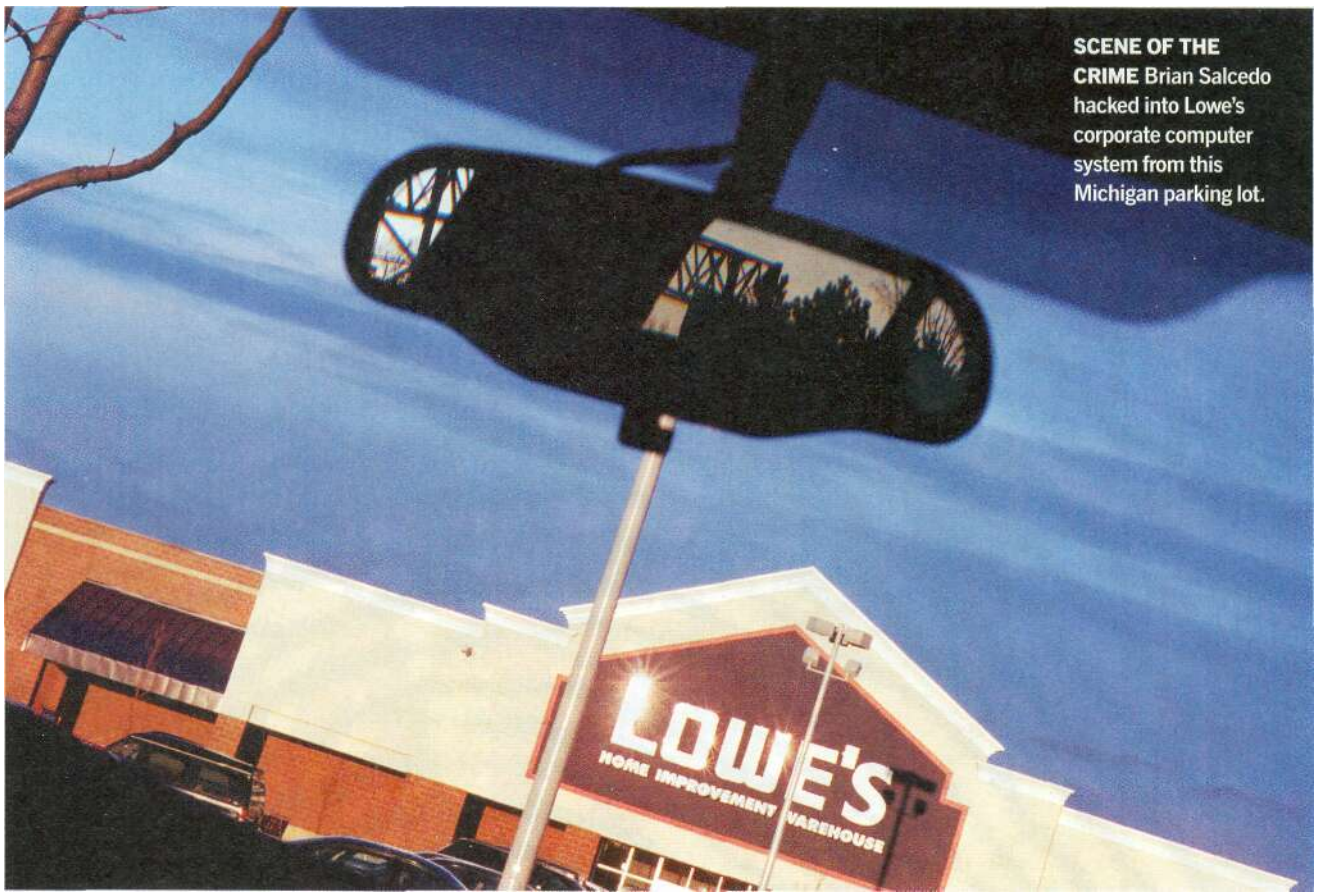
THE GREAT DATA HEIST

Why can't corporations keep their customers' personal data secure? Inside the world of identity theft. BY DANIEL ROTH WITH STEPHANIE MEHTA

The press release was written just seven months ago, yet it already sounds quaint. "U.S. announces guilty plea in largest identity-theft case in nation's history," declared the U.S. Attorney's office. The thief in question, a 35-year-old British immigrant named Philip Cummings, had admitted his central role in using information he had learned at work to pull off what the government declared to be "a massive scheme to steal the identities of up to 30,000 people."

Turns out Cummings was bush league. In February data aggregator ChoicePoint acknowledged that identity thieves had stolen vital information on 145,000 people. Less than two weeks later Bank of America admitted it had lost backup tapes that held the account information of 1.2 million credit card holders. In March shoe retailer DSW said its stores' credit card data had been breached; the U.S. Secret Service estimated that at least 100,000 valuable numbers had been accessed. More than a month later DSW released the real number: 1.4 million. Reed Elsevier's LexisNexis, a ChoicePoint rival, followed *suit*, revealing first that unauthorized users had compromised 32,000 identities, then upping the number to 310,000.

And those are just the headliners. Companies were ad-



SCENE OF THE CRIME Brian Salcedo hacked into Lowe's corporate computer system from this Michigan parking lot.

mitting scores of smaller breaches. On April 8, the San Jose Medical Group announced that someone had stolen one of its computers and potentially gained access to 185,000 patient records. A few days later customers of Polo Ralph Lauren learned that a hacker had gained access to 180,000 HSBC credit cards used at its stores. Then, on April 20, Ameritrade blamed its shipping vendor for losing a backup tape containing personal information on 200,000 clients. The Privacy Rights Clearinghouse, a nonprofit group in San Diego, estimates that some four million people's identities have been compromised since mid-February alone. Even more chilling, many of the bad guys appear not to have cashed in on their booty yet; they may be hoarding it to use later.

Corporate America is finally owning up to a long-held secret: It can't safeguard some of its most valuable data. Over the past few years, cheaper database software and storage devices have made it much easier for companies to gather and save private information about their customers, presenting a tempting (and surprisingly easy) target for identity thieves looking to do one-stop stealing and giving companies numerous ways to screw up security. A recent survey by the FBI and Computer Security Institute found that between 2000 and 2003 (the latest data available), about 40% of all companies confronted an attempted information snatch each year.

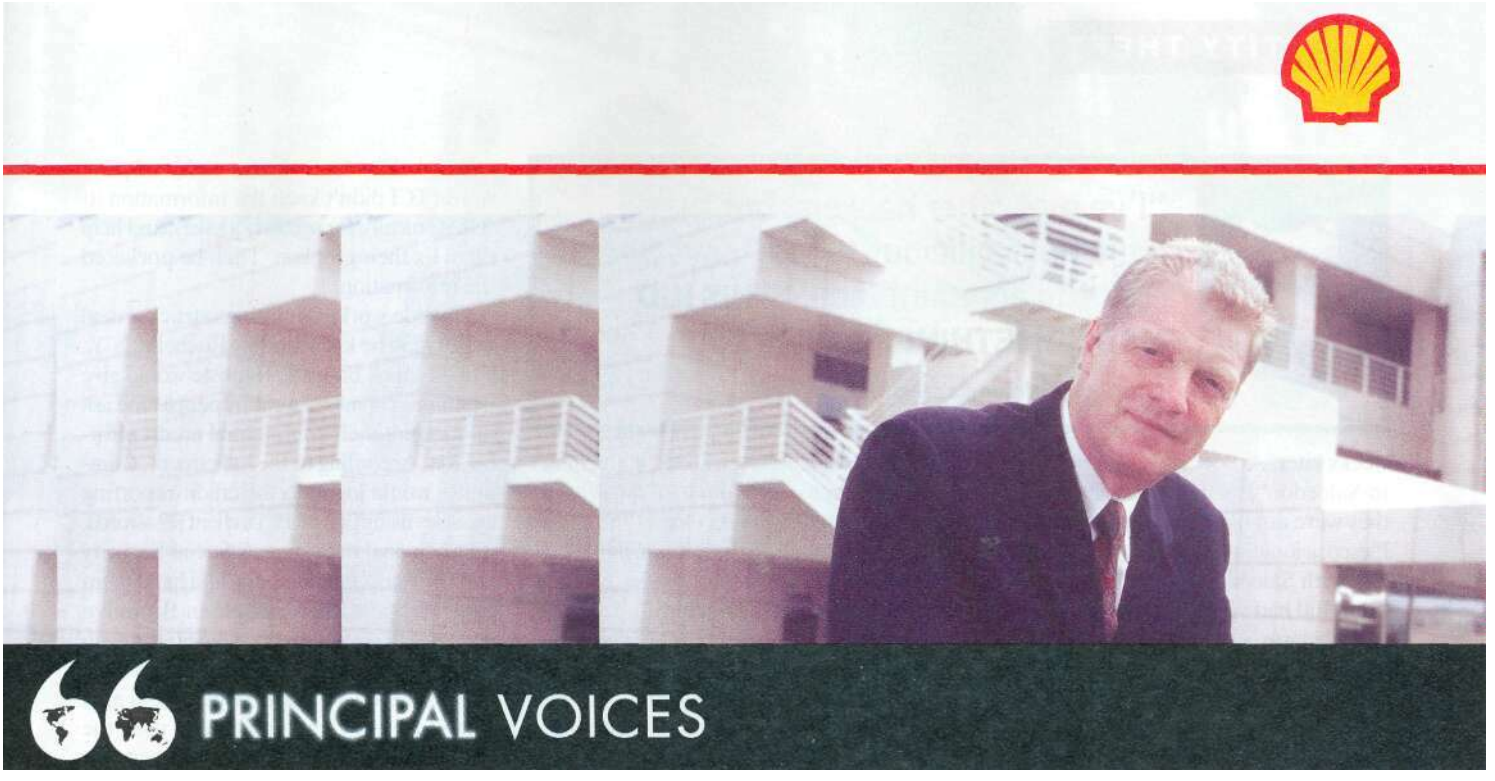
If data theft has been a constant plague, why the barrage of headlines now? Credit a California law, effective in mid-2003, requiring firms to notify its citizens when their confidential, non-encrypted information has been breached (for more on data-guarding laws, see "What's the Government Doing?"). What started as a slow trickle of mea culpas turned into a flood. Andrew Jaquith, a senior analyst covering security at Yankee Group, calls it "privacy's *Jerry Springer* moment."

Executives hoping to avoid joining in should beware: Boosting spending on IT security alone won't help. Secure information typically walks out the door in one of three ways: hackers grab it, employees steal it, or companies lose it—through incompetence, poor gatekeeping, bad procedures, or some combination of the three. High tech allows the data to be captured, but tech isn't always the way it escapes. To understand why companies are having so much trouble keeping their data secure, FORTUNE took a close look at two cases that led to long jail time—and two that are just now playing out.

THE HACKERS

On the evening of Nov. 7, 2003, two 20-year-old computer geeks named Adam Botbyl and Brian Salcedo pulled into the parking lot of a Lowe's home-improvement store in Southfield, Mich. From the comfort of Botbyl's white Pontiac Grand Prix, the duo opened a Wi-Fi-equipped laptop and logged on to a wireless access point meant for Lowe's employees to connect phones and scanners to the store's computer system. Once Salcedo and Botbyl had hopped onto the company's network, they tried to install a jury-rigged version of Lowe's credit-card-processing program. Their aim: to capture the credit card numbers of thousands of Lowe's customers.

They knew what they were doing. In 2000 Salcedo, then 17, showed up at a board meeting for Arbornet, a nonprofit online service provider based in nearby Ann Arbor, and identified himself as "the person who had hacked Arbornet." Attendees thought he was joking. But a few



PRINCIPAL VOICES

NAME: Sir Ken Robinson **PROFESSION:** Expert on education, the arts and creativity in business

Sir Ken Robinson was born in Liverpool in 1950. In 1981 he gained a PhD from the University of London for research into drama and theater in education. In 1998 he was appointed chair of the British government's National Advisory Committee on Creative and Cultural Education, and has served as adviser to a succession of high-profile public and private organizations. He was knighted in June 2003 for his outstanding achievements.

CREATIVITY IN THE CLASSROOM, INNOVATION IN THE WORKPLACE

What should be the role of bus/ness and industry *in the education of today's youth, and what strategies can realistically be put in place by business now to foster innovation on the widest possible range of platforms?*

Businesses everywhere have to compete in a world that's changing faster than ever. To keep pace they need people who can generate new ideas and adapt to constant change. Many companies say it's getting harder to find these people. One of the major reasons is education.

Most national systems of education weren't designed to promote creativity: their purpose was conformity. They prioritized the subjects that seemed most relevant to working life: mathematics, languages and science.

Two factors have changed all of this: the emergence of the knowledge economy and the demand for intellectual labor, and population growth. For both reasons, the numbers of people in education are expanding exponentially. As a result, the value of academic qualifications and skills are tumbling. Companies now face an unusual crisis in graduate recruitment. It's not that there aren't enough graduates to go around, it's that too many of them can't communicate, work in teams or think creatively. So, what can companies do to promote creativity for themselves?

The starting point is to challenge misconceptions. The first being that only special people are creative. Companies everywhere perpetuate this myth by dividing the workforce into the "creatives" and the "suits." Companies that are serious about innovation develop the creative capacities of all their people, not just "the creatives."

The second is that creativity is only about certain activities like advertising, design and marketing. Creativity is possible in all areas of our lives and essential in every aspect of business. The best companies innovate everywhere: in products, services and everyday systems.

The third is that you're either creative or not, and that there's not much you can do about it. The fact is that companies can do a lot to make creativity systematic, even routine - provided they know how.

Creativity is the process of having original ideas: innovation is putting them into practice. The most creative companies recognize this in how they recruit, position and train all their staff, not just a few. Personal creativity is stimulated by the ideas of other people: this is why innovative companies are constantly reforming creative and often cross-disciplinary teams.

Levels of organizational creativity are affected by three factors: habits - how people relate and work with each other; habifafs - the physical environment in which they work; and operating systems the management processes that support the business. Each can inhibit creativity and each can be changed to promote it.

We are living in times of revolution. Young people leaving school in 2005 may be retiring in 2050. They're likely to change occupations several times. Many will have jobs that haven't been invented yet, in businesses we can't imagine. To prosper, in every sense, we need radical, not reactive change in education.

It's in the direct interests of business to get involved in education reform. Individual businesses should engage in creative partnerships with schools and colleges to exchange expertise and ideas, and to support efforts to reform at a local level.

It's often said that education is the key to the future. It is. However, a key can be turned in two directions. Turn it one way and you lock resources away: turn it another and you release them. We won't survive simply by doing better what we have done in the past. In the future, we must learn to be creative.■

For more information on Sir Ken Robinson visit www.time.com/principalvoices or tune-in to the CNN Principal Voices series. In association with Shell.

Principal Voices is an international *project aimed at stimulating discussion on some of the more compelling challenges confronting our world today.*

"I've met other hackers, but they were not malicious types," says a Salcedo acquaintance. **"THIS KID HAD SOMETHING TO PROVE."**

WIRELESS Salcedo got caught hacking Lowe's.

weeks later, Arbornet went down, thanks to Salcedo. "I've met other hackers, but they were not malicious types," says Todd Plesco, a longtime Arbornet volunteer, who met with Salcedo at length in June 2000. "This kid had something to prove."

Botbyl was a shy giant of a man—he's 6 feet 5 inches tall—who once described himself on his personal weblog as a geek with a bad childhood. Salcedo apparently met Botbyl through local computer circles, and the two became friends. In the spring of 2003, Botbyl and another friend were "war-driving"—hunting for vulnerable Internet access points—around Southfield with a wireless-enabled laptop when they discovered a soft spot. A few months later Botbyl returned to Lowe's, this time with Salcedo, who tunneled his way into the company's network.

Over a period of several days Salcedo gained access not only to the Southfield store but to Lowe's corporate data center in North Carolina. Once inside, he learned how the retailer approved and processed credit cards, then wrote his own version of Lowe's proprietary credit-card transaction software. In Salcedo's version, according to a later indictment, the information would be saved in a file that he could later access.

What Salcedo apparently didn't realize is that many corporate computer systems are getting better at telling when someone's messing with them. Lowe's network engineers, from the company's data center in North Carolina, were able to piece together the timing of the various break-ins. Then, to Lowe's credit, it sought help. On Nov. 6, 2003, Lowe's officials called the Charlotte office of the FBI. Doris Gardner and members of her cybercrime squad arrived at Lowe's data center almost immediately. Agents took their places around the edge of the room while the Lowe's tech staff sought to zero in on the origin of the break-ins.

Using system-monitoring tools, the Lowe's team soon determined a security breach was happening that very moment in Southfield. On Nov. 7, Gardner had agents stake out the store there. For all the agents knew, the culprits could have been anywhere: tucked between aisles, in the men's room, on a loading dock. That evening the FBI caught a break. One of the agents needed to use the ladies' room, and as she was walking toward the Lowe's store, she noticed an eerie glow coming from the front seat of a Pontiac Grand Prix. It was the laptop. The FBI ran the license plate and came up with Botbyl's name.

Within days the geeks had been caught—before they were able to capitalize on any credit card information. Botbyl, 21, pleaded guilty to one count of conspiracy and is serving a two-year sentence. Salcedo, 22, was sentenced to nine years. Today he sits in a prison in Lewis Run, Pa. That's lucky for corporate America: The FBI says he hacked other companies that didn't stop him in time. "He definitely gained financially from other hacks," says the FBI's Gardner.

THE ROGUE EMPLOYEE

If Botbyl was caught by Lowe's security, shouldn't strong intrusion detection be enough to stop data leakage? Not by a long shot. Witness Teledata Communications—a company that prided itself on its security—and its problems with onetime employee Philip Cummings. In 1999, Cummings landed a job with TCI as a lowly help-desk worker. The company, now in Hauppauge, N.Y., makes devices used by banks, doctor's offices, and car dealerships that allowed instant credit checks by connecting to credit agencies like Experian or Equifax. When customers had problems logging on to one of the agencies from a TCI box, they would call in for help. Cummings would answer, ask them for their user code and password (TCI didn't keep the information itself, ironically, for security's sake), and help them fix their problem. Then he pocketed the information.

Outside work, Cummings struck a deal with a man he knew in New Rochelle, N.Y., named Linus Baptiste. Baptiste would give Cummings names of wealthy people and ask him to pull their confidential credit information. According to the indictment, Cummings would log in to the credit-reporting agencies using one of TCI's client passwords, find personal data such as Social Security and bank account numbers, and hand them over. Baptiste knew people in Brooklyn and the Bronx willing to pay $60 for each name; he and Cummings split the cash.

One of Baptiste's data buyers was a man named Eniete Ukpong. Ukpong used the pilfered personal information to open new credit card accounts, then went on spending sprees in New York and New Jersey. To turn the merchandise into cash, Ukpong would pass it off to yet another conspirator, Ahmet Ulutas, who sold many of the goods overseas. To those in the scheme, Ulutas went by two nicknames: "the Turk," because he was Turkish (he showed up in court with a Turkish translator), and "Pizza Guy," because (you guessed it) he worked at a pizza place—called Pizza Place.

The conspirators may not have been imaginative with nicknames, but they did have some good ideas about how to run a fraud. Cummings soon quit TCI and in 2001 moved to Georgia, where his moonlighting became a full-time job. He and Baptiste worked off a stolen TCI laptop and a roster of TCI client passwords. When a TCI client changed passwords, Cummings would move down his list, find another, and give it to Baptiste. Prosecutors say the two accessed some 30,000 names, all of which they sold to others. They continued doing that for two years; TCI never had any idea.

What's most troubling about the Cummings case is the low-tech nature of the crime. Cummings didn't have any partic-

"We do screening," says Cummings's former employer, **"BUT IT'S VERY HARD TO STOP A BAD APPLE."**

SMALL POTATOES Cummings sold each name for $60.

(TOP) MECKLENBURG COUNTY SHERIFF'S OFFICE; LOUIS LANZANO—LANDOV

ular computer skills; he just knew what he needed to take from his employer, and he knew people who could convert the information into money.

The first inkling of Cummings's doings, according to court documents, came in early 2002, when Ford Motor, one of TCI's clients, couldn't account for 15,000 credit checks that Experian said the company had made with it. When Experian checked Ford's records, it noticed that unusually large batches of consumer information had also been ordered by Washington Mutual Bank in Florida and by one other company. Soon the FBI was involved. Experian kept digging, as did Equifax. Both found that the requests seemed to be originating from one number in New Rochelle—a number that had at times called in using the account information of TCI customers like Dollar Bank in Cleveland and the Sarah Bush Lincoln Health Center in Mattoon, Ill.

On Oct. 29, 2002, FBI agents raided Baptiste's home and found three computers under two beds and credit reports hidden all over his bedroom. The agents also met with TCI president and co-founder Bill Nass and asked for a list of past and present employees. With Baptiste's help, the feds eventually fingered Cummings. "We were devastated," says Nass. "We do background screening, checking of people, but it's very hard to stop when you've got someone who's a bad apple."

Last fall Ukpong, Ulutas, and Cummings pleaded guilty to their roles in the crime. (Baptiste did the same in early 2003.) Cummings is now serving a 14-year sentence in federal prison. He declined to comment. Meanwhile, Nass has changed the way closely held TCI does business. The company no longer asks for subscriber passwords over the phone; customers must deal directly with the credit-reporting agencies. And TCI now sells a suite of software that lets companies screen their employees—software it developed after the Cummings incident. Says Nass: "It's been quite successful."

UNDER FIRE Weak safeguards enabled Olatunji Oluwatosin (below) to steal ChoicePoint data. Now CEO Derek Smith is on the hot seat.

CHRIS KLEPONIS—LANDOV

THE COMPANY SCREWUPS

"That seems beyond comprehension to me that that happened with one of the biggest banks in the country," said Senator Jim Bunning (R-Kentucky). It was mid-March, and he was grilling Barbara Desoer, a Bank of America executive vice president, in a Senate Banking Committee hearing. "Five, maybe ten, but 1.2 million [accounts]?"

Here's the story: In late December, Bank of America employees packed up and sent to its backup data center tapes containing information on government workers enrolled in a charge-card account. Or at least, that's where they were supposed to go. The tapes—none of which were encrypted—shipped via commercial air. But just after New Year's, bank officials realized that the tapes had never arrived. They scrambled to see what might be lost. It wasn't pretty: more than a million names, addresses, account numbers, and Social Security numbers. On Jan. 10 the bank called in the Secret Service.

For the next month the bank and the investigators worked in silence. Account holders had no idea that their information might be on the loose. Bank of America says the Secret Service asked it to keep quiet while it investigated. The bank kept monitoring the accounts, looking for any funny business, but found none—and still hasn't, it says. In mid-February the bank finally went public, promising that it had changed its ways (backup tapes no longer go by commercial air, for instance) and offering free credit reports and fraud monitoring to affected consumers.

Bank of America might have escaped serious damage, but security experts were left gasping at what it calls its "industry standard" methods of backing up and shipping customer data. "The Bank of America incident was absolute stupidity," says Jim Stickley, the CTO of TraceSecurity, a threat-management company based in Baton Rouge.

Stickley's main job is to break into banks, posing as a fire marshal, bug exterminator, or worker who has stepped out for a smoke break. Once inside, he helps himself to backup tapes, places keystroke detectors—good for capturing user names and passwords—on workers' computers, or installs a Wi-Fi access point in the server room, allowing him to get all the data he wants as he lounges in his laptop-equipped van in the parking lot. Banks actually pay him for this to see just how vulnerable they are.

Even though Stickley has seen plenty of gaping security holes, he can't stop talking about Bank of America. "Everything you

REPORTER ASSOCIATES *Mia Boorstin, Joan Levinstein*

Says CEO Smith: **"THE SECURITY BREACH AT CHOICEPOINT** has caused us to go through some serious soul-searching."

SCAM MAN Oluwatosin created phony businesses.

LOS ANGELES COUNTY SHERIFF'S OFFICE

want to protect is on those tapes. If they're not encrypted, strike No. 1. Then they're using commercial carriers to transfer the tapes, and they're like, -Everybody does that.' But that's not the case. It's not like it's a surprise that stuff can be stolen from commercial airlines. I think there were several bad choices they made there that could have been avoided." Alexandra Trower, a spokeswoman for the bank, defends its practice and the bank's follow-up: "We are continuing as we always do to look at our policies and procedures." She adds, "This is not a security breach like ChoicePoint."

Ah, ChoicePoint, enemy No. 1 to privacy advocates. Since spinning off from credit bureau Equifax in 1997, it has been buying up databases and data-mining operations. Businesses, individuals, even the FBI now rely on its storehouse. Other customers: Nigerian scammers who apparently used the data to rip off people's identities.

The problem was unreliable safeguards. To ensure that only certain businesses had access to its data, ChoicePoint set up certain requirements that potential customers must meet. A man named Olatunji Oluwatosin—and possibly others—used fake names and a Hollywood copy shop fax machine to create fictitious small businesses requesting ChoicePoint service. Before Oluwatosin was caught—after someone at ChoicePoint grew suspicious about one of his applications—he accessed at least 145,000 names. (Oluwatosin pleaded no contest to felony identity theft in California in February; he is serving a 16-month sentence.)

ChoicePoint hasn't gotten off easy either. After news of the data breach leaked out, ChoicePoint's stock hit the rocks, dropping from about $45 to a late-April low of about $37. At least three class-action suits have been filed, including one by the feared Bill Lerach, who accuses the company of concealing material information and of allowing executives to sell $20 million worth of ChoicePoint shares before the news broke. ChoicePoint declined to comment on the suits. But CEO Derek Smith, in prepared testimony before the House Energy and Commerce Committee, declared, "The security breach has caused us to go through some serious soul-searching."

It's too bad the soul-searching didn't happen earlier. After ChoicePoint revealed the breach, the company admitted that it had suffered a similar incident in 2001. But it never bothered reporting that one. F

FEEDBACK *droth@fortunemail.com*

WHAT'S THE GOVERNMENT DOING?

NEXT COME LAWS: Senator Patrick Leahy (left) grills LexisNexis CEO Kurt Sanford last month.

MANUEL BALCE CENETA—AP

Three key laws are meant to protect consumers from identity theft—but they aren't getting the job done. That's why two new ones (which may wind up being combined before they come up for vote) were introduced last month. Here's a look. — *Julia Boorstin*

FEDERAL LAWS

Gramm-Leach-Bliley Act (Financial Services Modernization Act): Aimed at financial companies. Requires those corporations to tell their customers how they use their personal information and to have policies that prevent fraudulent access to it. Partial compliance has been required since 2001.

Health Insurance Portability and Accountability Act: Aimed at the health-care industry. Limits disclosure of individuals' medical information and imposes penalties on organizations that violate privacy rules. Compliance required for large companies since 2003.

STATE LAWS

California's Notice of Security Breach Law: If any company or agency that has collected the personal information of a California resident discovers that non-encrypted information has been taken by an unauthorized person, the company or agency must tell the resident. Compliance required since 2003. (Some 30 other states are considering similar laws.)

PROPOSED FEDERAL LAWS

Schumer-Nelson ID Theft Bill: Would regulate companies that sell personal data, setting rules to prevent fraudulent access to information and requiring companies to disclose breaches in their security and the sale of personal information.

Notification of Risk to Personal Data Bill: A broader, nationwide version of California's security-breach law that carries tougher penalties for offending companies. Proposed by Senator Diane Feinstein of California.

Fonte: Fortune, v. 151, n. 8, p. 56-63, 16 may 2005.