

.....  
Date April 23, 2007

**RESOLUTION APPROVING: i2 CONTRACT FOR LAW ENFORCEMENT INTELLIGENCE DATABASE**

WHEREAS, this matter was brought before the City Council on the April 9, 2007 Roll Call No. 07-665, Council Communication No. 07-201; and,

WHEREAS, the City Council postponed this item to the April 23, 2007 Council Meeting in order that further information could be obtained for Council review; and,

WHEREAS, the City of Des Moines, Iowa Police Department is using a number of unsupported and disparate databases and large numbers of paper files to collect and store criminal intelligence information; and,

WHEREAS, the City of Des Moines, Iowa Police Department has no capability to incorporate open source information, or to query against the totality of the information, or to share the information horizontally across public safety agencies and those in the private sector with a need to know, or vertically among local, regional, state or federal agencies; and,

WHEREAS, the City of Des Moines, Iowa Police Department has a continuing need to exchange information and interact with Iowa Department of Public Safety's Intelligence Bureau, Fusion Center Hub and Law Enforcement Intelligence Network (LEIN), Iowa Department of Corrections, Midwest High Intensity Drug Trafficking Area (HIDTA) and the Mid-states Organized Crime Information Center (MOCIC) on a real time basis; and,

WHEREAS, the entities and agencies identified use i2's products for the entry and submission of criminal intelligence information, security, inquiry, dissemination, and review-and-purge processes in accordance with Federal Code of Regulations (28 CFR Part 23) "*Criminal Intelligence Systems Operating Policies*" and Iowa Code Chapter 692 "*Criminal History and Intelligence Data*"; and,

WHEREAS, the City of Des Moines entered into; Agreements with Iowa Homeland Security and Emergency Management Division for administration of Law Enforcement Terrorism Prevention Program funds to support the operation of the Region 5 Fusion Center and Intergovernmental 28E Agreements with Metropolitan Advisory Council (MAC) member communities for funding and implementation of Homeland Security Services; and,

WHEREAS, Municipal Code section 2-726 (a)(7) provides for a non-competitive procurement of goods and/or services that are of such a nature that they are the only goods and/or services which will fit and comply with the required use, or are an integral part of a total system so as to be uniquely compatible with existing city need, materials or equipment to be cost effective; and

NOW, THEREFORE, BE IT RESOLVED by the City Council of the City of Des Moines, Iowa, that the i2 Contract, dated March 26, 2007 for software program licensing, implementation services and maintenance is hereby approved and the Mayor of the City of Des Moines, Iowa is hereby authorized and directed to sign said Contract and the City Clerk is hereby authorized and directed to attest to the Mayor's signature and the Chief of Police is directed to carry out the terms and conditions of the Contract and to purchase the computer hardware and operating system required to develop and operate the law enforcement intelligence database.

★ Roll Call Number

Agenda Item Number

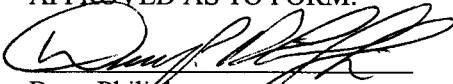
63

Date April 23, 2007

(Council Letter Number 07-244 attached)

Moved by \_\_\_\_\_ to adopt.

APPROVED AS TO FORM:



Doug Philip  
Assistant City Attorney

COUNCIL ACTION	YEAS	NAYS	PASS	ABSENT
COWNIE				
COLEMAN				
HENSLEY				
KIERNAN				
MAHAFFEY				
MEYER				
VLUSSIS				
TOTAL				

MOTION CARRIED

APPROVED

\_\_\_\_\_  
Mayor

**CERTIFICATE**

I, DIANE RAUH, City Clerk of said City hereby certify that at a meeting of the City Council of said City of Des Moines, held on the above date, among other proceedings the above was adopted.

IN WITNESS WHEREOF, I have hereunto set my hand and affixed my seal the day and year first above written.

\_\_\_\_\_  
City Clerk

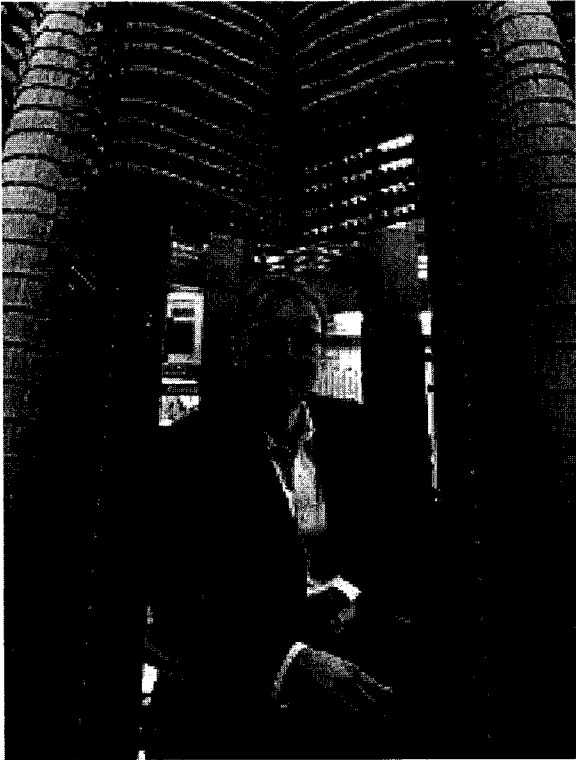
[http://www.nytimes.com/2006/11/12/business/yourmoney/12choice.html?\\_r=1&ref=technology&oref=slogin](http://www.nytimes.com/2006/11/12/business/yourmoney/12choice.html?_r=1&ref=technology&oref=slogin)

## Keeping Your Enemies Close

By Gary Rivlin, November 12, 2006

**The New York Times**

Alpharetta, Ga.



Darryl Lemecha, chief information officer at ChoicePoint, helps track client accounts for suspicious activity.

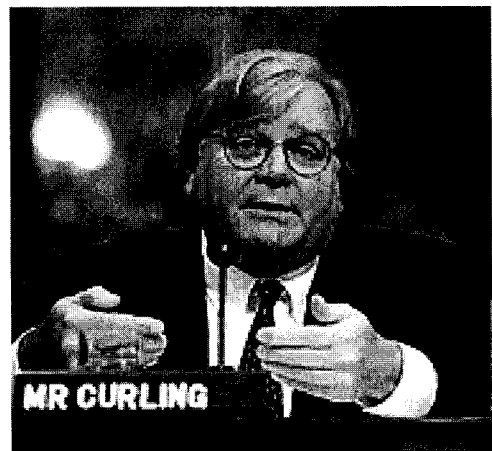
IF you found yourself running a company suddenly branded one of the most reviled in the country — if, for example, you noticed that visitors to Consumerist.com, a heavily visited consumer Web site, voted yours as the second “worst company in America” and you had just been awarded the 2005 “Lifetime Menace Award” by the human rights group Privacy International — you might feel obliged to take extraordinary steps. You might even want to reach out to your most vocal critics and ask them, “What are we doing wrong?”

So it was in early 2005 that Douglas C. Curling, the president of ChoicePoint, a giant data broker that maintains digital dossiers on nearly every adult in the United States, courted two critics whom he had accused just months earlier of starting “yet another inaccurate, misdirected and misleading attack” on his company.

Mr. Curling also contacted others who had spent years calling for laws requiring better

safeguarding of personal information that ChoicePoint and other data brokers assemble — records such as Social Security numbers, birth dates, driver’s license numbers, license plate numbers, spouse names, maiden names, addresses, criminal records, civil judgments and the purchase price of every parcel of property a person has ever owned.

“It was sort of like when I talk with my wife when she’s not happy with me,” Mr. Curling said of his dealings with some of ChoicePoint’s harshest critics. “It’s not exactly a dialogue I look forward to, but I can’t deny it’s important.” He also could not deny his motivations for engaging in these conversations: in the public’s mind, ChoicePoint



Douglas C. Curling, ChoicePoint president, on Capitol Hill in May 2005. He said a dialogue with critics was not pleasant but important.

had come to symbolize the cavalier manner in which corporations handled confidential data about consumers.

In January, the Federal Trade Commission hit ChoicePoint with a \$10 million fine, the largest civil penalty in the agency's history, for security and record-handling procedures that violated the rights of consumers. Under the settlement, it also required ChoicePoint to set aside an additional \$5 million to help those suffering financial harm because of its failure to provide adequate safeguards against data breaches.

But the financial penalties were nothing compared to the rehabilitation project confronting this hitherto invisible player in the global marketplace.

For years, ChoicePoint's top management had assured the world that it carefully protected its databases from intruders: Our systems are bulletproof. Intruder-proof. Believe us.

But then, in February 2005, the company had to acknowledge that it had focused so intently on preventing hackers from gaining access to its computers through digital back doors that it had simply overlooked real-world con artists strolling unnoticed through the front door.

Ultimately, ChoicePoint found that in 2005 alone, more than 40 phony businesses — thieves masquerading as bill collectors, private investigators, insurance agents and the like — had opened accounts that gave them unfettered, round-the-clock access to the vital data ChoicePoint maintains.

And, suddenly, the same privacy advocates that ChoicePoint had generally cast as shrill and ill-informed — a group that those inside the F.T.C. sometimes refer to as the "privacy posse" — proved crucial to its plans to both shore up its security and tend to its tattered image.

"I have to give them a lot of credit," said Daniel J. Solove, a posse member in good standing who had long been counted as one of ChoicePoint's most persistent critics. Mr. Solove, an associate professor at the George Washington University Law School, is among those whom ChoicePoint contacted shortly after its public relations debacle crested. "ChoicePoint had the attitude: 'We want to make our privacy practices exemplary,'" Mr. Solove said. "They wanted to find out what kinds of things they could do better and get feedback about some of the ideas they were thinking about."

For ChoicePoint, said James Lee, the company's chief marketing officer, the entire episode has proved an important learning experience. "The reality is, we were never as evil as people thought we were," Mr. Lee said, "but we were never as good as we thought we were."

Inside ChoicePoint, situated in a leafy office park in this suburb north of Atlanta, employees whistle with wonder over the talents of the various con artists — or "fraudsters," as company executives tend to call them — who finessed their way into their systems. According to the company, the fraudsters were wise enough to secure business licenses, thereby lending them a patina of legitimacy. They knew precisely what to write on their applications to convince ChoicePoint that their credentials made them fit for access to its databases.

"These guys were more sophisticated than anyone thought," Mr. Lee said, echoing the sentiment of many inside the company.

But the F.T.C. seemed to reach the opposite conclusion in a 33-page report it released earlier this year, after it completed an investigation of ChoicePoint. The commission found that ChoicePoint ignored "obvious red flags" because the company "did not have reasonable procedures to screen prospective subscribers." The report cast ChoicePoint's criminal

interlopers as sloppy and amateurish — but ultimately successful because their prey, a major company in the business of handling sensitive information, was alarmingly lax in its protection of its data repositories.

Signs that it was amateur hour inside ChoicePoint abounded, according to the F.T.C. report. The fraudsters faxed applications to ChoicePoint from a neighborhood Kinko's, listed post office boxes as primary business addresses and offered cellphone numbers as sole telephone contacts — which no one at ChoicePoint ever bothered to call anyway to establish the numbers' legitimacy. In at least one case, an approved applicant failed even to provide a last name, the F.T.C. found.

As ChoicePoint executives say, the fraudsters sometimes took the trouble to register their businesses with the state — but those documents should have set off alarms rather than justify the granting of an account.

The F.T.C. found that ChoicePoint accepted articles of incorporation that had been suspended or had expired, and "tax registration materials that showed that the business' registration was canceled." Then there were the contradictory addresses in the submitted documents — discrepancies that ChoicePoint employees accepted "without conducting further inquiry to resolve the contradiction," according to the commission's report.

"It was a well-known fact back then that ChoicePoint would do business pretty much with anyone who came along," said Robert Douglas, an information security consultant and editor of PrivacyToday who has done consulting work for ChoicePoint for several years. "They were making all the right noises about security but there wasn't any follow-through to back up their words."

Inside ChoicePoint, they like to say that the company is in the business of helping customers make informed decisions about whom they can trust.

Insurance companies and banks use its databases to help them decide who is a good credit risk and who is not. ChoicePoint sells its services to employers screening new hires, to landlords running background checks on new tenants, and to the 7,000 law-enforcement agencies and governments worldwide that the company counts as clients. Other customers include bill collectors, private investigators and media outlets, including The New York Times.

Yet a company with the snappy motto — "smarter decisions, safer world" — failed to use its resources to assess and then protect itself from some of its own customers. In some cases, the F.T.C. found, individuals were granted accounts "notwithstanding the fact that ChoicePoint's own internal reports on the applicant linked him or her to possible fraud." The company continued to furnish consumer reports to customers, the commission said, "even after receiving subpoenas from law enforcement authorities between 2001 and 2005 alerting it to fraudulent accounts."

Finally, in September 2004, ChoicePoint began to recognize that it had a major problem on its hands, when an employee in the company's new-accounts office realized that someone in the Los Angeles area, a Nigerian, was trying to set up multiple accounts, each time in the name of a different business.

The employee recognized the Nigerian's voice and alerted the company's security department, which in turn notified the local police. Although weeks would pass before senior executives learned of the troubling transactions with the Nigerian, the unfolding scam — and others like it — opened the eyes of outsiders to dangerous security lapses inside the company.

"I can assure you that now we learn immediately about this kind of problem," said ChoicePoint's chief executive, Derick V. Smith.

CHOICEPOINT was created in 1997 when Equifax, one of the big three credit reporting agencies — the others are TransUnion and Experian — spun off one of its divisions. Back then, the unit that would become ChoicePoint was involved in the labor-intensive and barely profitable business of maintaining claims histories on behalf of insurance companies. It also administered physicals, drug tests and the like for clients. Mr. Smith and Mr. Curling, who together ran what was then called the Insurance Services Group, foresaw a promising market in peddling data about individuals to a wider group of customers, and they convinced higher-ups that their unit should venture off on its own.

Since then, ChoicePoint has acquired more than 70 smaller companies and bought whatever databases it could get its hands on, including motor-vehicle reports from counties around the country, police records, property records, birth and death certificates, marriage and divorce decrees and criminal and civil court filings. These records had long been publicly available, but automation and superfast computers meant that comprehensive data dossiers could be assembled in seconds.

"It used to be that a business would have to go to 10 or 20 different vendors to get the same information that ChoicePoint sells in a single report," said Chris Jay Hoofnagle, a senior researcher at the Boalt Hall School of Law at the University of California, Berkeley, and a privacy advocate.

That approach has certainly proved lucrative. The company's stock price has quadrupled in nine years, and its revenue has, too, topping \$1 billion in 2005. That growth has come despite stiff competition from two other companies of similar size that market background information about ordinary Americans: Acxiom, a publicly traded company based in Little Rock, Ark., and the LexisNexis Group, a division of Reed Elsevier. Many smaller companies are also in the business.

ChoicePoint sees itself as playing an essential, if not noble, role in the information economy. It has — at a reduced rate — helped nonprofits working with children identify registered sex offenders who applied for jobs, and it has provided the data that allowed the police to track down hundreds of missing children. Mr. Curling and others inside ChoicePoint argue that if there were no data brokers, home loans would take that much longer to secure and insurance rates would be based not on a person's driving record but on broad demographic categories, such as age and gender. Sure, breaches have been a problem, but theirs is still a young industry, ChoicePoint executives say.

"It takes time to establish best practices," Mr. Smith said.

It also took a state law. The data thieves who conned their way into ChoicePoint's system downloaded information about at least 166,000 individuals. In years past, the company would alert law enforcement officials when it suffered a data breach, according to Mr. Lee, and leave it at that. But under a California disclosure law passed in 2003, the company was required to notify every Californian whose personal details might have fallen into criminal hands.

"No one knows for sure, and no one can say, how many breaches occurred before California," Mr. Hoofnagle said. "This is an 'known unknown,' as Donald Rumsfeld would say."

RATHER than send letters only to the 42,000 Californians whose records had been downloaded by the fraudsters, ChoicePoint mailed a notice to all affected consumers, telling them that their

personal information might have fallen into the hands of identity thieves. Critics chided ChoicePoint for waiting about five weeks to contact consumers, but the company said it first needed to set up and staff a call center to handle the anticipated deluge of complaints.

"We knew that in all likelihood the first time that they were ever going to hear of ChoicePoint was in this letter," Mr. Lee said.

That would hardly be the last they would hear of ChoicePoint, however. Over the coming months, a long list of corporations and governmental agencies took their turn in the spotlight after they were obliged to acknowledge fumbling people's personal data: LexisNexis, Bank of America, Time Warner, Boeing, the Department of Veterans Affairs. And with each new breach, media accounts invariably mentioned the company whose breach had spurred a great awakening about the vulnerability of every individual's personal data — even if that company, ChoicePoint, had nothing to do with the other companies' woes.

Privacy critics were initially dubious when ChoicePoint contacted them in the wake of its February 2005 announcement. "Most gave us the Heisman," said Mr. Lee, who held out his forearm like a running back pushing away a would-be tackler to demonstrate his point. Yet, over time, most though not all of the privacy posse would agree to meet with Mr. Curling and other ChoicePoint executives, and walk away impressed by what they heard and saw.

That would include Professor Solove at George Washington ("They've implemented quite a number of measures to protect privacy"), Chris Hoofnagle at Berkeley ("ChoicePoint now has model security practices") and Beth Givens, director of the Privacy Rights Clearinghouse, a consumer advocacy group based in San Diego ("They've put in place practices that I wish all the data brokers would adopt").

Senator Charles E. Schumer, Democrat of New York, became an honorary member of the privacy posse when he declared the F.T.C. overly lenient for levying only a \$10 million fine against ChoicePoint. But he, too, has changed his tune.

"I was worried that a fine would be seen as the cost of doing business," Mr. Schumer said in an interview. "But I have to say, ChoicePoint has become a model company."

Even Marc Rotenberg, a privacy posse member who refused to meet privately with Mr. Curling or anyone from ChoicePoint out of concern that doing so would undermine his credibility, begrudgingly gave ChoicePoint some praise.

"While I'm prepared to give them credit for a series of positive steps, I don't think it would be accurate to say that they got to this position on their own," said Mr. Rotenberg, the executive director of the Electronic Privacy Information Center, a privacy rights group in Washington. "It took a lot of work by EPIC and other organizations."

When ChoicePoint started its makeover campaign, it first offered to rain down freebies on possible victims of identity theft, a protocol that others would follow. It invited them to join a credit monitoring service at no charge for one year, and provided them with free reports from the big three credit bureaus. To actual victims of identity theft, it offered its expertise to help correct the problem.

The company also gave a \$1 million, four-year grant to the Identity Theft Resource Center, a nonprofit group in San Diego.

ChoicePoint then overhauled its security measures, a move that began with the hiring of Carol A. DiBattiste, who ultimately would fill the new position of chief privacy officer. Ms. DiBattiste is a

no-nonsense lawyer whose résumé includes 20 years in the Air Force and turns as an assistant United States attorney. To send the message that both security and privacy were a priority, Ms. DiBattiste was named the company's general counsel one year into her tenure. Over the years, ChoicePoint had done a modest but lucrative business working with private investigators and other smaller enterprises. Shortly after its February 2005 announcement, the company said that it would no longer provide full Social Security numbers, birth dates or other sensitive information to these customers — data that Ms. DiBattiste called "keys to the castle."

That decision, Mr. Curling said, cost the company \$15 million to \$20 million last year. But inside ChoicePoint, executives saw that this small sliver of business threatened its overall reputation.

Until 2005, ChoicePoint had left credentialing to people in individual business units. It now has a centralized credentialing department. "The salespeople play no role in credentialing anymore," said Ms. DiBattiste, who deployed dozens of people to take on the painstaking chore of recredentialing every client that was not either a law-enforcement agency or a public company. ChoicePoint had 120,000 accounts before February 2005; it now has 104,000.

It also performs random audits of its customers, to ensure that they are conducting searches appropriate for their type of business, and it uses its computer systems to monitor accounts for suspicious activity.

"We look for any anomalies," said Darryl Lemecha, the company's chief information officer. "So if we see a 50-person company that typically does a background check like once a month suddenly do 20 in one day, we lock down that account so we can investigate."

ChoicePoint has endured roughly 100 outside audits, most of them conducted by long-term corporate customers, "and we passed them all," Ms. DiBattiste said. As part of its settlement, ChoicePoint agreed to submit to an F.T.C. audit every other year for the next 20 years.

It is not yet clear how many people were actually harmed by ChoicePoint's negligence. ChoicePoint says it knows of only 46 people who have been defrauded because of its data breach. But law enforcement officials have identified at least 800 people who have been identity theft victims because of ChoicePoint's missteps, said Betsy Broder, an assistant director at the privacy and identity protection unit of the F.T.C. But, she said, that number could rise.

"If data was stolen," Ms. Broder said, "nothing prevents the thieves from holding on to it for a period of time and using it perhaps when consumers let down their guard, or when the alert on their credit expires."

ChoicePoint also set up a Web site for consumers who, at no cost, want to check and challenge possible inaccuracies in their dossiers ([www.choicetrust.com](http://www.choicetrust.com)). "It's hard to overstate the significance of this,"

Ms. Givens said. "This is an important step forward in moving us to transparency."

Whether other companies follow suit remains to be seen. Michael Dores, founder of Merlin Information Services, a ChoicePoint competitor based in Kalispell, Mont., said he would offer free consumer reviews of its dossiers — but the cost, he said, "would put me out of business."

STILL, Mr. Dores said, ChoicePoint's own woes have had a big impact on Merlin, whose customers tend to be smaller businesspeople like debt collectors and private investigators. Like ChoicePoint, Merlin was fooled into providing an account to a fraudster.



So the company has recredentialed all its customers, Mr. Dores said, and created a new two-person compliance department. He said that Merlin now gives detailed personal data only to a small fraction of those to whom it provided such sensitive information in the past, much to the chagrin of many longtime customers.

Mr. Dores said he felt that he had no choice but to put these changes into effect, because “the Federal Trade Commission is in a bad mood over this stuff.”

Members of the privacy posse still have their complaints about ChoicePoint.

Roughly 60 percent of its business falls under the Fair Credit Reporting Act, which regulates the collection and use of consumer credit information.

But to Mr. Hoofnagle and other privacy advocates, that is not enough. “If I had a magic wand I would make all of ChoicePoint’s data fall under the Fair Credit Reporting Act,” Mr. Hoofnagle said.

Even so, those who previously reserved most of their criticisms for ChoicePoint now aim their harshest words at some of its competitors. The same private investigators and others who formerly obtained Social Security numbers from ChoicePoint and Merlin are now simply seeking the services of other data brokers — companies such as Tracers Information Specialists of Spring Hills, Fla.

Yet Terry Kilburn, the chief operating officer of Tracers, said he was not worried about the hazards of providing such sensitive information. “We weren’t the ones who were breached,” Mr. Kilburn said. “Our security and compliance are strong, and so we are choosing to continue to do business the way we always have.”

In Washington, legislators have proposed more than 20 bills to monitor data brokers more closely. According to Senator Schumer, ChoicePoint — in contrast to other large data brokers — has supported legislation he has proposed that would establish stricter security standards for any entity handling sensitive personal information.

“ChoicePoint, to its credit, got right behind our legislation and lobbied for it,” Senator Schumer said. But the bill, which he and Senator Bill Nelson, Democrat of Florida, introduced in April 2005, has not passed, he said, “because a lot of other companies, quietly and behind the scenes, killed it.”



## Who's guarding your data in the cybervault?

USA TODAY, Monday, April 2, 2007

In a remarkable turnaround, ChoicePoint, the giant data broker excoriated two years ago for its lack of precautions as it went about gathering and selling personal data, has recast itself as a model corporate citizen.

California's milestone data-theft disclosure law forced ChoicePoint in February 2005 to reveal that it had sold sensitive information for at least 166,000 people to a Nigerian con artist posing as a debt collector. The Federal Trade Commission hit ChoicePoint with a record \$10 million fine and ordered it to set aside \$5 million to aid data breach victims.

The once-obscure data broker, tucked away in a nondescript business park 20 miles north of Atlanta, also embraced extensive reforms. The result: ChoicePoint is regarded by a dozen leading privacy advocates interviewed by USA TODAY as the most responsible company among dozens in the lightly regulated, fast-growing field of aggregating and selling sensitive information.

"ChoicePoint transformed itself from a poster child of data breaches to a role model for data security and privacy practices," says Gartner analyst Avivah Litan.

Despite ChoicePoint's makeover, there's rising concern among privacy experts and legislators about the frenetic business of assembling and distributing personal data. Everyone, it seems, wants Social Security numbers, birth dates, maiden names, criminal records, civil judgments and real estate records. Lenders, landlords and employers want as much data as they can get their hands on to size up applicants; law enforcement officials want it to track down criminals and terrorists. And cybercriminals are boosting demand for personal information as they concoct new Internet-enabled scams.

Data brokers such as ChoicePoint and LexisNexis assemble names, addresses, property records and other public records for use by everyone from employers to law enforcement agencies.

The Big Three credit-reporting agencies — Equifax, Experian and TransUnion — have a narrower focus. They compile data about car loans, credit card debt, mortgages and more to determine credit scores for lending institutions.

With a patchwork of state laws on data handling in place — and most data brokers just beginning to take basic precautions — the average citizen increasingly faces a new kind of multi-tiered jeopardy, law enforcement officials and privacy advocates say. Identity thieves often muck up data dossiers, while data brokers have little incentive to emphasize security or accuracy.

"You and I as consumers don't even know where all this information comes from or how it gets corrupted, and we have no way to fix it," says Mari Frank, an attorney and privacy consultant. "You can be denied credit or a job; you can be totally defamed; and you have no way to access the data to fix it — that's what's scary about the lack of privacy in the information age."

### Scrutiny

Since its notorious data breach became public, ChoicePoint has imposed dozens of enhanced security policies. It has beefed up credentialing and auditing of customers and expanded an online service ([www.choicetrust.com](http://www.choicetrust.com) <<http://www.choicetrust.com/servlet/com.kx.cs.servlets.CsServlet?usertype=c>> ) that lets individuals view their own records and make corrections for free. To underscore its Fort Knox-like approach, 26 surveillance screens form a backdrop at a guard's station at the main entrance.

All told, the company, whose annual revenue quadrupled over the past decade and now tops \$1 billion a year, spent about \$14 million tightening operations. It also exited the highly profitable business of selling Social Security numbers, birth dates and driver's license numbers to private detectives, mom-and-pop collections agencies and other small-time clients, giving up \$15 million in annual revenue.

In a pivotal move, it recruited longtime Defense and Justice department official Carol DiBattiste to fill the new position of chief privacy officer and take over as general counsel at an annual compensation of about \$800,000. That's more than twice what her peers earn, says Ari Schwartz, a privacy advocate and deputy director of Center for Democracy and Technology.

DiBattiste has steered the company through more than 80 audits by government agencies and big corporate clients to review its security and privacy procedures. "Arguably we were the most audited company in 2005 and 2006," says the energetic DiBattiste.

Privacy advocates worry that self-policing isn't enough; only a portion of what data brokers do falls under the federal Fair Credit Reporting Act, which regulates how the Big Three collect and disseminate consumer credit histories.

Data brokers argue that much of what they disseminate is not covered by federal rules "because it is based on public records" such as birth and death certificates, and property records, says Evan Hendricks, editor of Privacy Times newsletter.

Chris Hoofnagle, senior fellow to the Berkley Center for Law and Technology at the University of California-Berkeley, contends modern-data storage and data-mining technology has allowed data brokers to pervert the intent of open records law. "The government compels individuals to reveal their personal information in

a variety of contexts, then pours it into the public record for anyone to use," he says. Data brokers "collect the information, repackage it and return it back to the government and businesses full circle."

#### A bad dream

Critics such as Pam Dixon, executive director of World Privacy Forum, rail against the data brokers' practice of selling vast quantities of personal data to government agencies. ChoicePoint says less than 4% of revenue comes from the sale of data to government customers, but it won't name them.

Accuracy of data flowing to employers and creditors is a big concern. Dixon says if consumers had access to all of the data ChoicePoint supplies to the government, that "would be a tremendous help in easing the harms stemming from data inaccuracies." Erroneous profile data disrupt people's lives every day, privacy experts say.

James Derrell White, 41, who happens to live in Alpharetta, Ga., where ChoicePoint is based, was denied a job with Home Depot this year because data provided by ChoicePoint incorrectly identified him as a felon. "We thought we were in a bad dream," says Julie White, James' wife.

The data broker intermingled data for White and a felon with the same name and birth date. After the office of U.S. Rep. Tom Price, R-Ga., contacted ChoicePoint on the Whites' behalf, the matter was resolved and White got the job. ChoicePoint says it was already resolving the matter.

(Last week, ChoicePoint started a pilot program to give job applicants the chance to view their criminal background report at the same time as their potential employer.)

ChoicePoint says that its core mission is to help companies and government agencies temper risks.

Company executives, including chief marketing officer James Lee, have taken to repeating a catch phrase about ChoicePoint's earnestness dealing with critics: "It's like facing your wife when she's angry; it's not fun, but you learn something."

#### Deluge of breaches

By attempting to take the high road in the freewheeling data-brokering trade, ChoicePoint has spotlighted how an unregulated industry can police itself, Hoofnagle and others say.

DiBattiste says she has heard rumblings that other companies think "we're 'doing too much.' "

ChoicePoint's initiatives have had the effect of deflecting criminals' attention to less-attentive data brokers, as well as to all organizations storing large caches of personal information, Dixon says.

More than 500 incidents ranging from TJX to the Department of Veterans Affairs have been reported, involving records lost for tens of millions individuals since 2005. Privacy Rights Clearinghouse started the Chronology of Data Breaches list after ChoicePoint went public with its breach in February 2005.

A flurry of breaches reported last December — UCLA, 800,000 records stolen; Aetna, 130,000; and Boeing, 382,000 — pushed the number of records that have turned up missing over the 100 million mark; it recently topped 150 million. Yet Daniel Solove, an associate professor at the George Washington University Law School, and other privacy experts say Acxiom and LexisNexis "act as if nothing happened."

Executives at Acxiom and LexisNexis rebut such criticism. "Everything ChoicePoint has done since 2005, we already offer," says Jennifer Barrett, chief privacy officer at Acxiom, which specializes in lifestyle data — information about the reading and voting habits of consumers culled from public records and consumer surveys. LexisNexis spokeswoman Sue D'Agostino said the company is "confident that our security procedures are as robust as others in the industry."

#### Extending the market

Newer data brokers, such as ZabaSearch <<http://zabasearch.com/>> , Intelius, PrivateEye.com <<http://www.privateeye.com/processor.asp?piid=46>> and Voompeople.com <<http://www.voompeople.com/processor.asp>> , have stepped up efforts to extend the market for profiles to everyday consumers. PrivateEye.com, Voompeople.com and ZabaSearch did not respond to interview requests.

These online services typically require payment by credit card for background checks of varying thoroughness. Intelius is a representative example: It supplies data you can get on yourself — or anyone else — simply by typing a first and last name. This will usually pull down your home address and age, along with similar data on relatives who share your surname, as well as strangers with similar names.

Intelius' core business: enticing consumers to run \$50 background checks on nannies, coaches, health care workers and the like.

Given transitory modern culture and the wide array of public records, inaccuracies are unavoidable, data brokers say. Inconveniences are offset by

peace of mind gained from verifying credentials, says Ed Petersen, Intelius vice president of sales and marketing.

Yet, more widely dispersed data also means more opportunity for criminals; identity thieves can secure sensitive data from the online brokers as easily as any consumer — and pay with stolen credit card numbers, says Idan Aharoni, senior fraud analyst at RSA, the security division of EMC.

Gartner estimates 15 million Americans will become victims of identity theft this year, up 50% from two years ago. "Since a fake ID is an integral part of most fraud operations, there are entire sections within the underground dedicated to forging IDs," Aharoni says.

Federal lawmakers, meanwhile, have begun to weigh in with proposed legislation.

Sens. Patrick Leahy, D-Vt., and Arlen Specter, R-Pa., would mandate consumers' rights to correct misinformation about them and allow federal agencies to assess the quality of data supplied by data brokers.

Sen. Dianne Feinstein, D-Calif., is seeking to ban the sale or display of people's Social Security numbers without their consent.

"No matter how good any company's attitudes toward privacy, there are too many players in the (data-collecting) industry — too many intricate parts when it comes to privacy issues — to expect self-regulation to effectively deal with the problems," Solove says.

Swartz reported from Alpharetta, Ga., Acohido from Seattle.





## ChoicePoint Privacy and Information Security Enhancements Fact Sheet

### I. Customer Access to Sensitive Personally Identifiable Information (SPII):

- **Exited Select Consumer-Sensitive Data Markets not covered by the Fair Credit Reporting Act.** ChoicePoint discontinued selling products that contain SPII (e.g., social security numbers and drivers' license numbers) in selected markets, at a cost of approximately \$15 - \$20 million in revenue.
- **Changed Process For Distributing SPII.** ChoicePoint no longer distributes information products that contain SPII except:
  - To support consumer initiated transactions such as insurance, employment and tenant screening, or financial
  - To provide authentication or fraud prevention tools to large accredited corporate customers where consumers have or want to establish relationships (e.g., fraud prevention tools for identity verification, customer enrollment and insurance claims)
  - To assist federal, state and local governments and criminal justice agencies

Even for these services the Sensitive Personally Identifiable Information and dates of birth may be masked from view, truncated or echoed (mirrored) back if provided by customers or consumers.
- **Remove Certain Non-SPII From Tenant Screening Reports to Further Reduce Potential Risk.**
- **Truncate SPII and Dates of Birth on Public Records (i.e., Civil and Criminal Returned From Public Record Sources) With Limited Exceptions.**
- **Restricted Resellers Access to Credit Data in Certain Background Screening Products.**

### II. Credentialing:

- **Established a Centralized Corporate Credentialing Center.**
- **Strengthened Customer Credentialing Procedures Utilizing Multiple Internal and External Sources and an Expanded Site Visit Program.**
  - Recredentialed existing customers regulated by the Fair Credit Reporting Act ("FCRA"), requiring:
    - Successful completion of credentialing process.
    - Certifications of permissible purpose.
    - Site visits (with limited exceptions) (site visit checklist, scoring and quality control review).
  - Credential new customers regulated by the FCRA, requiring:
    - Successful completion of credentialing process (checklist, scoring and quality control review).
    - Certifications of permissible purpose.
    - Site visits (with limited exceptions) (site visit checklist, scoring and quality control review).
  - Credential other customers not regulated by the FCRA, requiring:
    - Successful completion of credentialing process (checklist, scoring and quality control review).

- Site visits (with limited exceptions) for customers receiving SPII (site visit, scoring and quality control review).
  - Enhanced procedures for credentialing resellers.
- **Developed Third Party Service Provider (e.g., vendors) Program.** Created to help ensure that third-parties that have access to ChoicePoint-maintained personal information have appropriate privacy and information security safeguards in place. Third parties must complete a self assessment questionnaire that is reviewed and scored.
- **Enhanced Employee Credentialing Program and Implemented Employee Re-Credentialing Program.**

### **III. Policies, Procedures and Guidelines:**

- **Developed Information Security Breach Response and Consumer Notification Policy and Procedures.** ChoicePoint has developed a policy for response and notification to consumers in the event of a security breach.
  - Once relevant law enforcement agencies determine that notification of affected consumers will not impede a criminal investigation or threaten national security, ChoicePoint will notify the following parties in the most expedient time possible by appropriate means and in compliance with federal, state, and local laws and regulations:
    - The three major credit bureaus
    - Affected consumers
    - The Identity Theft Resource Center, a national nonprofit organization that assists victims of identity theft
    - Affected customers and businesses whose information was or is reasonably believed to have been compromised
    - Appropriate ChoicePoint information/data vendors whose information was or is reasonably believed to have been compromised
    - Government representatives and relevant federal, state, and local regulatory agencies, as appropriate
  - Policy sets forth assistance provided to consumers in the event of an information security breach
    - Toll-free number and website assistance to answer questions about incidents and assist affected consumers in taking the necessary steps to detect and protect against identity theft
    - One year of free credit monitoring which includes alerts of any key changes that may be a sign of identity theft
    - \$50,000 of identity theft insurance
    - Access to ChoicePoint fraud resolution representatives
    - Support from Identity Theft Resource Center

- **Codified, Enhanced and/or Developed (62) Other Key Policies, Procedures and Guidelines since January 2006. Examples include:**

○ Employee Access to ChoicePoint Information	○ IT User
○ Change Management	○ Laptop Physical Security
○ Code of Conduct	○ Non-US Internet Access
○ Corporate Incident Response	○ Physical Security
○ Corporate Records	○ Public Representations
○ Credentialing Center Customer Credentialing and Site Visits	○ Record Access Restriction
○ Customer User Access Security	○ Remote Access
○ Data Protection and Classification	○ Reseller and Other Third Party Data Access, Transfer, and Usage
○ Data Suppression/Truncation	○ Third Party Services Provider Information Security and Privacy Assessment
○ Employee Credentialing and Re-Credentialing	○ Web Site Privacy Policies
○ Information Security	

**IV. Audit and Compliance:**

- **ChoicePoint Successfully Completed 43 Third Party Audits in 2005 and 40 Audits in 2006:**
  - 2006 Audits included:
    - Several major insurance companies
    - A federal agency
    - A credit bureau
    - Major financial institutions
    - Other customers
    - 6 SAS70 Type II Reviews covering 17 applications. These reviews are technology process-oriented and focus primarily upon compliance with our internal controls over information security, computer operations, and application change control.
    - A comprehensive audit of ChoicePoint’s Information Security Program.
- **ChoicePoint Underwent a Comprehensive Independent Assessment of its entire Information Security Program From August to October 2006.**
- **Enhanced ChoicePoint’s Audit and Compliance Program.**
  - Engaged Ernst & Young LLP privacy team to assist in developing privacy compliance framework.
  - Increased compliance audit staff.
  - Automated customer and consumer audit processing.
  - Developed new insurance customer audit program.

- Enhanced reseller compliance audit program to include site visits and self assessment questionnaires.
- Developed compliance plans for over 60 internal policies and procedures to monitor compliance.
- Enhanced customer suspicious activity monitoring.
- 2006 audits completed:
  - FCRA customer permissible purpose
  - Consumer sampling verifying FCRA permissible purpose
  - Other non-FCRA customer permissible purpose
  - Mandatory training
  - Corporate Credentialing Center
  - Reseller
  - Web site privacy policies
  - ChoicePoint-initiated audits to monitor compliance with legal requirements and ChoicePoint internal policies and procedures

## **V. Organizational:**

- **Established Company-Wide Accountability for Privacy and Security.**
  - Created Security Advisory Committee (composed of senior leadership)
  - Created a Security Working Group (composed of key managers)
  - Created policy, risk and credentialing Sub-working groups
  - Created privacy and security positions within the business units to assist with implementation of privacy policies, compliance and privacy education
- **Established Office of Credentialing, Compliance and Privacy (“CCPO”).** The CCPO is headed by Carol DiBattiste, ChoicePoint’s General Counsel and Chief Privacy Officer. Ms. DiBattiste reports directly to the Privacy and Public Responsibility Committee of the Board of Directors of ChoicePoint on privacy matters.
- **Appointed Law Enforcement Liaison.** ChoicePoint appointed Robert McConnell, a 28-year veteran of the Secret Service and former chief of the federal government’s Nigerian Organized Crime Task Force, as its law enforcement liaison.
- **Established a Consumer Advocate Office.** This office fundamentally enhances our interactions with consumers in the following five key areas:
  - Consumer outreach
  - Consumer advocacy
  - Consumer assistance
  - Internal awareness
  - Consumer policy

## **VI. Technology Solutions:**

- **Enhanced Network Security.**
  - Ensured systemic implementation of technical standards, patch management, and anti-virus standards across the enterprise, resulting in no serious virus infections in 2005
  - Continued vulnerability assessment program by maintaining an average of 0 level 5 issues and fewer than 10 level 4 issues enterprise-wide

- **Implemented Application Scanning Services.** ChoicePoint implemented external web server scans and application scanning services to reduce risk and satisfy customer requirements.
- **Implemented Additional Encryption Technology.**
  - Implemented various technologies for secure messaging and encryption, to include enabling encryption technology for 20+ business processes, encryption of data feeds to credit bureaus, protection of mobile devices, and database encryption for multiple business units to protect millions of rows of sensitive consumer data. These include the following types of encryption:
    - Transport Layer Security (TLS)
    - Pretty Good Privacy (PGP)
    - Voltage Identity Based Encryption (IBE)
    - Laptop Hard Drive
  - Enabled our businesses to be compliant with Payment Card Industry standard using database encryption.
- **Developed a Data Classification Tool.** This tool is used to classify ChoicePoint data based on sensitivity.
- **Performing Monthly Password Assessments.** ChoicePoint's internal access team conducts assessments and notifies users when and how to strengthen passwords to protect from unauthorized access.
- **Acquired Tool For Scanning For SPII Data.** This tool proactively scans work stations and the network for SPII and assigns necessary protections and deletes data not needed.
- **Designed a Risk Management and Control Framework.** Framework will be used biennially for ChoicePoint risk assessments and tested to ensure appropriate physical, administrative and technical safeguards exist across the business units.

## **VII. Outreach and Education:**

- **Enhanced Privacy Principles/Policy Posted on [www.privacyatchoicepoint.com](http://www.privacyatchoicepoint.com).**
- **Created a Dedicated Privacy Web Site [www.privacyatchoicepoint.com](http://www.privacyatchoicepoint.com).**
- **Developed a ChoicePoint Privacy and Information Security Enhancements Fact Sheet, posted on [www.privacyatchoicepoint.com](http://www.privacyatchoicepoint.com).**
- **Created an Employee and Fraud Reporting Hotline: 866-473-3728.**
- **Created a Privacy Hotline: 877-301-7097.**
- **Developed and Implemented Enhanced Mandatory (annual) Online Training Programs, with Assessments:**
  - Privacy
  - Information Security Awareness
  - Code of Conduct
- **Created and Implemented Social Engineering Training For Specified ChoicePoint Associates.**
- **Members of CCPO Obtained International Association of Privacy Professionals Privacy Certification.**
- **Obtained On-Line Privacy Seals From TRUSTe for Consumer Oriented Web Sites.**
- **Instituted Program to Notify Stakeholders of Privacy Related Announcements.**

- **Partnered With The American National Standards Institute and the Better Business Bureau.** ChoicePoint along with eight other founding partners will develop Identity Theft Prevention and Identity Management Standards.
- **Changed Process to Enable Consumers to Request Information Available on [www.choicetrust.com](http://www.choicetrust.com).** Information can be ordered and delivered on-line for free. The information includes FCRA and FACT Act reports as well as public record searches.
- **Developed a Consumer-Oriented Video.** Designed to fully explain our background screening and insurance services businesses.
- **Created a “How to Read a Consumer Report” Tool For Customers and Consumers.**
- **Improved Consumer Dispute Resolution Response Times.**



### **Case Study: ChoicePoint Incident Leads to Improved Security, Others Must Follow**

Avivah Litan

ChoicePoint transformed itself from a "poster child" of data breaches to a role model for data security and privacy practices. One new practice involves careful credentialing of customers, a critical business process that should have standards — but doesn't.



## WHAT YOU NEED TO KNOW

---

The upside of ChoicePoint's data breach disclosure is that it drove the industry to improve security standards. Still, businesses engaged in data brokering and credit reporting have very uneven data privacy standards, and all should be held to the same standards as ChoicePoint is. The market will not likely address this issue without government intervention and/or regulations.

## CASE STUDY

---

### Introduction

In October 2004, ChoicePoint, an Atlanta-based data services provider, discovered it mistakenly issued user accounts to Nigerians posing as a legitimate small business. The scammers potentially gained access to some 140,000 consumer records in ChoicePoint's system. Ultimately, they were discovered by a ChoicePoint employee who recognized the voice of the scammer attempting to open accounts as different people. The company reported the suspicious behavior to local authorities, which arrested the individual with its cooperation. ChoicePoint was bound to comply with the nearly 18-month-old California Security Breach Notification Law, which required it to notify affected consumers that their information may have been compromised.

By February 2005, ChoicePoint's name was splattered across the press in the first of many — and more serious — breaches to be revealed under newly adopted state disclosure laws. With negative headlines widespread, the market cap of ChoicePoint, with \$918 million in 2004 annual revenue and more than 50,000 business customers, dropped 22% in the ensuing three months. The U.S. Congress convened hearings on the data brokerage and credit industry's practices in managing sensitive customer data. Until then, ChoicePoint had been growing its business at a healthy rate of more than 10% a year, but suddenly it became a household term associated with identity theft.

Fast-forward two years to September 2006. Some 80 million U.S. adult accounts have been potentially compromised, 34 states have passed information breach notification laws similar to California's, and ChoicePoint has now become a role model for protecting customer data privacy. To find out how ChoicePoint managed this turnaround, Gartner spoke with key players involved in this project.

### The Challenge

Following an investigation by the Federal Trade Commission (FTC), ChoicePoint agreed, in January 2006, to pay a \$10 million fine and to spend \$5 million for consumer redress. In addition, the company complied with an injunction for up to 20 years for some provisions, stating that it had to:

- Credential its customers that are regulated by the Fair Credit Reporting Act (FCRA) (still ChoicePoint includes non-FCRA-regulated customers in its credentialing program)
- Inspect certain of its customers' facilities
- Conduct independent audits
- Submit to extensive monitoring by and reporting to the FTC

ChoicePoint recognized that it needed to tighten its data-handling practices. After all, it has access to information on nearly every U.S. adult resident, obtained from every level of

government as well as private-sector sources, such as credit bureaus, white pages directories and other commercial providers. Business customers rely on ChoicePoint services for a variety of critical functions, ranging from employee screening, homeland security compliance and mortgage processing to home, auto and commercial insurance policy underwriting.

In April 2005, ChoicePoint embarked on strengthening its data security and privacy program. Its goals included:

- Better knowing its own business customers
- Operating transparently with consumers
- Creating a framework of enhanced controls for its business

## Approach

ChoicePoint adopted a controls framework based on industry standards, where they existed, and it created its own standards where they did not. The company's privacy policy is based on the American Institute of Certified Public Accountants' Generally Accepted Privacy Principles (<http://infotech.aicpa.org/Resources/Privacy>), and its security policy is based on ISO 17799. In terms of customer credentialing — a critical business process and the area involved in its data breach — ChoicePoint created its own standard.

ChoicePoint focused on five main areas to achieve its goals: organizational governance, credentialing, technology, training and compliance, as described in the following sections. Through June 2006, the company's expenses directly related to the fraudulent data access totaled nearly \$30 million.

### Organizational Governance

ChoicePoint's first action after its well-publicized incident was to hire a Chief Credentialing, Compliance and Privacy Officer (CCCPO), who reports to the Privacy and Public Responsibility Committee of the company's board of directors. The CCCPO is tasked with oversight of the data privacy program and is directly responsible for compliance and auditing of ChoicePoint customers and the credentialing processes. The CIO now owns the operation of information security, customer support and the credentialing programs. The senior managers work through two company working groups. Each functional business area is tasked with security responsibilities, with representatives serving on a working group.

### Credentialing

With limited exceptions, ChoicePoint researches every business requesting a customer account, performing due diligence, including site visits to prospective customers. It utilizes an extensive credentialing checklist as well as a separate site visit checklist, the details of which remain confidential because of the matter's sensitivity. Physical site inspections validate the legitimacy of the customer and the security of the customer's premises, which enables ChoicePoint to reconcile the customer's application with physical observations.

Fortune 500 companies are the easiest to credential because much information on them is readily available. Credentialing smaller companies, which have scarce historical data and references, is more problematic. Here, ChoicePoint found an inverse revenue-to-cost structure — many smaller customers were unprofitable to its business. Hence, ChoicePoint made a deliberate decision to exit certain business areas, such as those in which customers could not be credentialed in a low-risk yet profitable manner.

- ChoicePoint requires customers to certify that they will use ChoicePoint data for only permissible purposes.

#### Third-Party Service Providers

- ChoicePoint requires its resellers and third-party service providers (contractors) to complete a self-assessment of their data security practices. This self-assessment consists of 25 questions covering subjects from employee training to data disposal methods and user access. Failure to submit self-assessments may result in the immediate termination or suspension of the customer's ChoicePoint account, pending the outcome of an investigation.

#### Audits

- ChoicePoint randomly audits customers on a daily basis to determine if they are using ChoicePoint data for permissible purposes.
- ChoicePoint samples consumers on a daily basis to ensure company customers obtained the required permission before requesting a report on the consumer.
- ChoicePoint randomly audits resellers and third-party service providers to determine if they maintain adequate privacy and security safeguards.

Failure to abide by ChoicePoint's policy, as uncovered by the audits, may result in the immediate termination or suspension of customer accounts, pending an investigation's outcome.

#### Technology

##### Data Management

- All files and applications were inventoried to fully understand what data is processed and to apply the right protections to the application.
- Random machines are periodically audited for selected personally identifiable information (PII) to ensure sensitive information is properly secured. While ChoicePoint does not share information on what tools it uses, it evaluated solutions from Tablus and Vontu.
- ChoicePoint developed a data classification tool that recommends data protection and retention requirements.

##### Encryption

- ChoicePoint implemented database encryption on its credit card payment processing engines in early 2005 (as it became compliant with the Payment Card Industry standard). Given the low number of credit card accounts maintained by the company (fewer than 10 million), ChoicePoint opted for a tactical, software-based approach after evaluating both hardware solutions and native database encryption. The company evaluated vendors such as Ingrian and Protegrity and the native Oracle encryption. It implemented column-level encryption using a Protegrity product, which was transparent to the application as well as to the database schema (the software automatically decrypts the sensitive information on query). Credit card numbers are rarely used as indexes, so this method proved easy, inexpensive and secure.
- ChoicePoint instituted various options for encrypting transmitted data, including HTTPS, and e-mail encryption using either mail-server-to-mail-server encryption (Transport Layer Security) or through Pretty Good Privacy clients distributed to clients who handle significant amounts of PII data. It also implemented an automatic encryption product that can encrypt any e-mail with sensitive data in it, as detected by ChoicePoint's regular expression-based content monitoring and filtering engine on its mail server.

- ChoicePoint is on plan for a full-scale rollout of laptop hard-drive data encryption by the end of 2006.

#### Data Truncation

ChoicePoint decided to truncate all sensitive PII data sent to customers so that they cannot view full social security, credit card, driver's license or other sensitive account numbers. This rule holds unless the data distribution meets three criteria:

- An end user gives prior approval for having data sent; for example, during pre-employment screening.
- The data is used by an antifraud application.
- The data is being delivered to law enforcement.

ChoicePoint competitors do not employ the same data truncation practices, which gives them an advantage because many customers don't want to bother with truncated data. This points to the important need to establish uniform data privacy standards across the data brokerage and credit-reporting industry.

#### Activity Monitoring

ChoicePoint has implemented different monitoring systems that provide early warnings of potentially fraudulent activity. For instance, access from non-U.S. IP addresses is blocked to certain products. A Web session analysis engine is used for certain products to detect events such as multiple logins from the same user account, logins that are physically in two different places within a short period of time and other anomalies. Other engines watch for unusual activity, such as sudden increases in the number of queries, queries that are too fast to reasonably be done by a person typing on a computer; or query patterns that are not typical for a specific employment-related activity.

#### Training

Early in the third quarter of 2006, ChoicePoint rolled out a mandatory online privacy training program for all permanent and temporary employees and independent contractors who research court records. A second information security awareness program was also recently introduced. Employees are tested annually for successful completion of both programs and must score at least 80%.

In August 2006, ChoicePoint rolled out social engineering training programs for call center employees so that they don't fall victim to various techniques fraudsters use over the phone.

#### Compliance

ChoicePoint holds its assistant vice president of information security accountable for system security, and the company audits systems periodically (weekly, biweekly or after major application changes) by performing vulnerability assessments and network and application scans. The internal audit staff manages financial and Sarbanes-Oxley Act compliance. The CCCPO audits customers, resellers, third-party service providers and the Corporate Credentialing Center, and also monitors internal policy compliance.

The company's primary focus is auditing its customers — it audits a certain percentage of its accounts annually. In accordance with the FTC order, ChoicePoint audits a sample of consumers served by the audited companies to ensure that the consumers had given permission to those companies to order their consumer reports.

## Results

### ChoicePoint

The company implements embedded high-priority data security and privacy practices throughout its organization.

- It publicly reported specific expenses addressing the data breach incident totaling \$27.3 million in 2005 and \$1.8 million through 30 June 2006. Ongoing operational costs resulting from the changes the company made are now included in its normal cost structure.
- It implemented a best-of-breed credentialing program that partially relies on physical site visits, illustrating the fact that a risk-based layered security approach is most effective.
- In 2005, the company lost nearly \$20 million in business because of its deliberate decision to stop doing business with customers whose credentials could not be thoroughly validated.
- It became one of the most-audited companies in the U.S. in 2005: It underwent 43 third-party audits, five of which were SAS 70 audits of the company's applications. In 2006, ChoicePoint expects to complete up to 30 audits, including a particularly grueling one required by the FTC.

## Critical Success Factors

The company took advantage of a crisis to make fundamental changes to conduct its business more securely.

New data security projects were driven and sponsored by ChoicePoint's chairman, president and the board (notwithstanding the FTC order, and the fact that its survival depended on it).

The entire company became involved in understanding, implementing and ensuring compliance with the new privacy and security agenda. The process was not restricted to only a few divisions.

Appropriate training and awareness programs were implemented for all employees, from the highest-level executives to associates at all levels.

To achieve transparency, business leaders fully engaged in the details of the business's practices and interested external parties were fully informed as to how ChoicePoint operates.

## Lessons Learned

- Business transparency is critical, especially when you are a custodian of confidential consumer data.
- Credentialing customers involves many nuances, and credentialing most smaller, unknown business customers with little transaction history is generally not worth the effort or the cost.
- Audit, compliance and training are critical tools to ensure people and organizations follow through on stated objectives and practices.
- The market lacks standards in customer credentialing, which is a critical area that must be addressed to prevent fraud.
- Considerably more work is required to change the business culture and practices than to implement security technology applications.

## REGIONAL HEADQUARTERS

---

**Corporate Headquarters**

56 Top Gallant Road  
Stamford, CT 06902-7700  
U.S.A.  
+1 203 964 0096

**European Headquarters**

Tamesis  
The Glanty  
Egham  
Surrey, TW20 9AW  
UNITED KINGDOM  
+44 1784 431611

**Asia/Pacific Headquarters**

Gartner Australasia Pty. Ltd.  
Level 9, 141 Walker Street  
North Sydney  
New South Wales 2060  
AUSTRALIA  
+61 2 9459 4600

**Japan Headquarters**

Gartner Japan Ltd.  
Aobadai Hills, 6F  
7-7, Aobadai, 4-chome  
Meguro-ku, Tokyo 153-0042  
JAPAN  
+81 3 3481 3670

**Latin America Headquarters**

Gartner do Brazil  
Av. das Nações Unidas, 12551  
9º andar—World Trade Center  
04578-903—São Paulo SP  
BRAZIL  
+55 11 3443 1509



63



Midwest High Intensity Drug Trafficking Area  
 Iowa State Program Coordinator  
 709 E. 2<sup>nd</sup> Street  
 Des Moines, Iowa 50309  
 Phone (515) 281-9354 Fax (515) 281-9056

November 20, 2006

Len Murray  
 Des Moines PD  
 25 E. 1<sup>st</sup> St.  
 Des Moines, IA 50309

Dear Mr. Murray:

Midwest HIDTA analysts, including Iowa's analyst, utilize the software Notebook to link subjects in drug investigations. The information is then shared with other departments to assist in investigations with common links.

The analysts at the ISC, Intelligence Service Center, in Kansas City also utilize the software in analysis of information from drug investigations through out Midwest HIDTA.

Dennis Wilbur  
 Iowa State Program Coordinator  
 Midwest HIDTA





Regional Information  
Sharing Systems

# Mid-States Organized Crime Information Center®



1610 E. Sunshine ♦ Suite 100 ♦ Springfield, MO 65804  
(417) 883-4383 ♦ WATS: (800) 846-6242 ♦ FAX: (417) 883-1532

December 13, 2006

Major L. Murray  
Des Moines Police Department  
#25 East 1st Street  
Des Moines, Iowa 50309

Dear Major Murray:

I was contacted by our Iowa field coordinator, Wayne Lunders, who stated that you are considering the purchase of the i2 Software.

MOCIC has used this program for many years with each of our analysts having a license for the software. As a matter of fact, an i2 trainer is currently conducting a 3-day training course in our office. This training will be beneficial to both our experienced analysts and to the one that we have just hired.

In view of your request for information about the software, I asked the trainer about their installed base. She indicated that they have over 2,000 federal, state, and local governmental agencies in the United States that are using their product. In addition, she indicated that fusion centers are either already using the software or are considering purchase. Private corporations are also using the software. Our experience has been that many agencies are using the i2 Software for their analytical work. Due to our investment in the software, we have been able to exchange files with those agencies in cases of mutual interest. Although the i2 Software is not the only software we use for case analysis, it has become an integral part of our arsenal.

If you have additional questions in regard to this software, please do not hesitate to contact me.

Sincerely,

Bill Goodrich  
Deputy Director



**Sole Source Letter**

11/14/06

Mr. Len Murray  
Des Moines PD  
25 East 1<sup>st</sup> St.  
Des Moines, IA 50309

i2 is the publisher, holder of all copyrights, and holder of sole source for the software and maintenance and support listed below. Furthermore, i2 is the exclusive distributor of these products. Portions of our products are protected by trade secrets and are unique in the market. These i2 specific software packages must be purchased directly from i2 at the address listed on this letterhead.

**Products, Maintenance & Support**

- |  |                      |
|--|----------------------|
| i2 Analyst's Notebook ®                | i2 iBridge Developer |
| i2 Analyst's Notebook ® French         | i2 iBridge           |
| i2 Analyst's Notebook ® Spanish        | i2 iBridge French    |
| i2 Analyst's Notebook ® German         | i2 iBridge Spanish   |
| i2 Analyst's Notebook ® Developers Kit | i2 PatternTracer TCA |
| i2 Analyst's Workstation               | i2 Visual Notebook   |
| i2 iBase Designer                      | i2 iXv               |
| i2 iBase                               | i2 iXa               |
| i2 iBase Designer SSE                  | i2 Text Chart        |
| i2 iBase SSE                           | i2 Chart Explorer    |
| i2 iBase GIS                           |                      |

If you desire additional information, do not hesitate to contact us toll free at (888) 546-5242 or locally at (703) 921-0195 at any time or visit our website at [www.i2inc.com](http://www.i2inc.com). Thank you for your interest in our products.

Jack Reis  
President  
i2 Inc.

i2 Inc. is an award-winning company that develops data visualization and link analysis software for investigations and intelligence operations. i2's advanced analytical tools are used in law enforcement, intelligence, defense, military security, insurance, and many Fortune 500 companies. i2 products are currently in use in over 100 countries worldwide and are widely recognized as the industry standard.

SOLE SOURCE JUSTIFICATION

The contract for visual investigative analysis software being entered into by the Department of Public Safety (State) and i2 Inc., (Vendor) is being done without the process of accepting bids for this service for the following reasons.

1. i2 software creates charts that show complex information in a new light, highlighting significant entities or links which would otherwise be missed.
2. DPS already owns one copy of the software, Analyst Notebook. Also, the Iowa Department of Corrections also owns several copies of this as well as iBridge. This project would help in the sharing of information between State agencies.
3. The contractor, i2 Inc., is the only known vendor that provides this type of product that is designed to integrate with Oracle which is the database the LEIN Intelligence database is designed in.
4. License cost for the Analyst Notebook software has been negotiated to a significant reduction in price from \$4,784 price per copy to \$3,659 each. This is a total saving of \$4,500 to the State of Iowa.
- 5.

**Bill Kroes**  
System Manager  
Intelligence Bureau  
Iowa Department of Public Safety  
(515) 281-3010 Fax- (515) 281-6108



63

**Rauh, Diane I.**

---

**From:** Jones, John L.  
**Sent:** Wednesday, April 18, 2007 2:34 PM  
**To:** Rauh, Diane I.  
**Subject:** FW: ChoicePoint Information for meeting



ChoicePoint Privacy Gartner Case Study  
and Inform... 091906.pdf



NY Times  
111206.doc



USATodayArticle04  
0207.doc

-----Original Message-----

**From:** Elaine Clevenger [mailto:Elaine.Clevenger@i2inc.com]  
**Sent:** Saturday, April 14, 2007 4:29 PM  
**To:** Murray, Leonard L.; Jones, John L.  
**Cc:** Kevin Moore  
**Subject:** ChoicePoint Information for meeting

John and Len,

In response to certain statements about ChoicePoint made by a representative of the American Civil Liberties Union during the Des Moines City Council meeting on April 9, 2007, ChoicePoint would like to provide the following information.

ChoicePoint (NYSE: CPS) is a company committed to helping its corporate, government and non-profit customers identify and mitigate risk. The bulk of our work is with the insurance industry helping underwriters, e.g., Nationwide and State Farm, price home and auto insurance specific to an individual consumer rather than across a broad class. According to the insurance industry, these efforts result in 70% of Americans receiving lower priced insurance. Our second largest business works with tens of thousands of employers - large and small - to perform pre-employment background checks on their potential employees. As a part of this effort, we work with thousands of non-profits around the country to help them screen their volunteers. In Iowa last year we did more than 50,000 of these non-profit background screens at steeply discounted cost. Every week we find convicted sex offenders looking to work with children or other at-risk populations. As for our work with the government, we are primarily a supplier of technology like the one sought by your police department. This software is used around the world to stop crime and capture criminals.

Security breaches are not unique to ChoicePoint. Other entities that have experienced security breaches include the Iowa Department of Education, the University of Iowa, Iowa Student Loan, Iowa State University, the University of Northern Iowa, JP Morgan Chase & Co., CitiFinancial, Ford Motor Co., TJX, Bank of America, Money Gram International, and Kaiser Permanente. A report of 2007 information security breaches was released on April 12, 2007, by the Identity Theft Research Center, which states that already this year 76 breaches have occurred affecting over 54 million consumers. Said breaches have occurred in the following areas: government/military; educational; medical/healthcare; and banking/credit/financial.

The security breach that ChoicePoint disclosed in early 2005 was not a hacking incident. Criminals falsified documents and posed as legitimate businesses to obtain access to certain, not all, ChoicePoint products. Moreover, our incident was by no means the largest data breach. The fact is that we provided notice to fewer than 170,000

individuals who may have been affected by this incident. The number of individuals actually affected is estimated by various government agencies to range from about three dozen to as high as 1,000 consumers. The only certain number of which we are aware, however, is the less than 40 victims who have been identified in publicly filed indictments against the convicted ID theft criminals.

In the days and weeks following ChoicePoint's data breach incident, the company undertook a series of steps to identify and address the areas of its security, privacy and credentialing that needed to be enhanced. With this came an unprecedented level of internal and external scrutiny, not just of the company's business practices but of the customers of the company as well: ChoicePoint's customers were asked to undergo a re-certification process that included site visits to their primary places of business. This effort involved ChoicePoint's senior leadership and resulted in a vastly improved public perception of the company's commitment to protecting personally identifiable information from misuse. The above mentioned enhancements along with others in the areas of technology, policy, audit and compliance and outreach and education have been captured in ChoicePont's Privacy and Information Security Enhancements Fact Sheet (attached).

There have been several positive articles published that speak to ChoicePoint's commitment to privacy and information security. The New York Times and USA Today have recently published articles (attached). Both reflect that ChoicePoint has, in fact, transformed itself in the words of one independent analyst from a "poster boy" to a "model" corporate citizen. This quote was taken from a Gartner case study of ChoicePoint (attached). The USA Today story's headline was "ChoicePoint Redeems Itself."

While ChoicePoint's efforts have been recognized as leading practices in the industry, being good stewards of protecting consumer privacy and information is a continuing endeavor and one that ChoicePoint takes very seriously.

Thank you,

Elaine Clevenger

Vice President

i2/ChoicePoint Government Services

(888) 545-5242 office

(703) 203-1234 cell

www.i2inc.com <<http://www.i2inc.com>>

-----  
The information contained in this e-mail message is intended only for the personal and confidential use of the recipient(s) named above. This message may be an attorney-client communication and/or work product and as such is privileged and confidential. If the reader of this message is not the intended recipient or an agent responsible for delivering it to the intended recipient, you are hereby notified that you have received this document in error and that any review, dissemination, distribution, or copying of this message is strictly prohibited. If you have received this communication in error, please notify us immediately by e-mail, and delete the original message.