HISTORY
CONTEXT
Even if you understand the past you are doomed to repeat it.
That’s called “human nature”.
And while the past informs the future, it’s called the future for a reason.
Local 338, International Longshoreman's Association
Aug 22, 1953

700 Records
Computer hackers steal code to credit rating bureau system

90,000,000 Records
Dear Customer,

Egghead.com has discovered that a hacker has accessed our computer systems, potentially including our customer databases. While there is no indication that any customer information has been compromised, as a precautionary measure, we have taken immediate steps to protect you by contacting the credit card companies with whom we work. They are in the process of alerting card issuers and banks so that they can take the necessary steps to ensure the security of cardholders who may be affected.

We wish to underscore that we have taken these steps as precautions. We have no information at this time to suggest that any credit card information has been compromised. We are investigating this possibility, and we are doing everything we can to proactively protect you. If you would like further information, you may wish to contact the issuer of your credit card to determine what steps they are taking. We regret any inconvenience this may cause you.

We issued a press release on this matter earlier today. [...] If you have additional questions, please call our customer service team at 1-800-EGGHEAD (344-4323).

Respectfully,

Jeff Sheahan, President & CEO, Egghead.com, Inc.

Friday, 22 December, 2000
What We Know

• Egghead.com detected an intrusion on December 18th.
• They contracted Kroll on December 21st and notified the credit card companies.
• Egghead.com notified 3.7 million customers on December 22nd. Card issuers began canceling and re-issuing cards.
• After a 20 day investigation, it was believed no credit card information was lost. Fraud levels were not unusual.
• Egghead.com filed for bankruptcy on August 15th, and was acquired by Amazon on November 26th.
What We Learned

• Most people assumed Egghead.com went out of business due to this breach.

• It inspired a (short) generation of secrecy.

• Analysis of their business metrics revealed that the company was in decline due to mismanagement long before the breach.
We learned the wrong lesson.
Playboy
Nov 20, 2001

Ziff-Davis
Nov 20, 2001

"Hundreds" of credit cards

Experian/Ford Motor Credit Company
Jan 1, 2002

13,000 Full Credit Reports
And promptly ignored
The law of data breaches

Businesses suffer from breaches even if customers don’t suffer from fraud.
Virginia Credit Union  
May 7, 2003

California SB 1386 Operative  
Jul 1, 2003

PetCo  
Jul 12, 2003
Unusual activity detected on 50 small business accounts
Sep 27, 2004

Olatunji A. Oluwatstin, a 41-year-old Nigerian national, arrested with 5 cell phones and 3 credit cards.
Oct 27, 2004

Media reveals ChoicePoint suffered similar breach in 2002.
Mar 2, 2005

“A Nigerian-born brother and sister were charged in 2002 with a scam in which they posed as legitimate businesses to set up ChoicePoint accounts and gain access to its massive database. They then made 7,000 to 10,000 inquiries on names and Social Security numbers in the database and used some of those identities to commit at least $1 million worth of fraud. Assistant U.S. Attorney Mark Knuse in Los Angeles said yesterday.”

Final class action lawsuit filed for $50
Jan 28, 2008

ChoicePoint suffers another breach
Oct 11, 2008

1.3 million people exposed after they discovered poor identity.
4 months with no upgrading (IC) from Choice.
Requires additional alterations reporting.
Unusual activity detected on 50 small business accounts
Sep 27, 2004

Olatunji A. Oluwatosin, a 41 year-old Nigerian national, arrested with 5 cell phones and 3 credit cards.
Oct 27, 2004

Media reveals ChoicePoint suffered similar breach in 2002.
Mar 2, 2005

“A Nigerian-born brother and sister were charged in 2002 with a scam in which they posed as legitimate businesses to set up ChoicePoint accounts and gain access to its massive database. They then made 7,000 to 10,000 inquiries on names and Social Security numbers in the database and used some of those identities to commit at least $1 million worth of fraud, Assistant U.S. Attorney Mark Krause in Los Angeles said yesterday.”
"A Nigerian-born brother and sister were charged in 2002 with a scam in which they posed as legitimate businesses to set up ChoicePoint accounts and gain access to its massive database. They then made 7,000 to 10,000 inquiries on names and Social Security numbers in the database and used some of those identities to commit at least $1 million worth of fraud, Assistant U.S. Attorney Mark Krause in Los Angeles said yesterday."

ChoicePoint reveals problem not limited to California
Feb 16, 2005

35,000 California residents notified
Feb 8, 2005

38 state Attorneys-General demand notification
Feb 19, 2005

ChoicePoint states an additional 10,000 people affected
Feb 21, 2005

Total later raised to 163,000.
ChoicePoint limited scope of investigation to July 1, 2003.

Final class action lawsuit settled for $100M
Jan 18, 2008

ChoicePoint suffers another breach
Oct 19, 2009
13,750 people exposed after bugs discovered in ProductHunt

Remember this date
Jul 1, 2003
Remember this date

Jul 1, 2003

35,000 California residents notified
Feb 8, 2005

ChoicePoint reveals problem not limited to California
Feb 16, 2005

38 state Attorneys-General demand notification
Feb 19, 2005

ChoicePoint states an additional 110,000 people affected
Feb 21, 2005

Total later raised to 163,000.

ChoicePoint limited scope of investigation to July 1, 2003.
Media reveals ChoicePoint suffered similar breach in 2002.
Mar 2, 2005

“A Nigerian-born brother and sister were charged in 2002 with a scam in which they posed as legitimate businesses to set up ChoicePoint accounts and gain access to its massive database. They then made 7,000 to 10,000 inquiries on names and Social Security numbers in the database and used some of those identities to commit at least $1 million worth of fraud, Assistant U.S. Attorney Mark Krause in Los Angeles said yesterday.”
Media reveals ChoicePoint suffered similar breach in 2002.

Mar 2, 2005

“A Nigerian-born brother and sister were charged in 2002 with a scam in which they posed as legitimate businesses to set up ChoicePoint accounts and gain access to its massive database. They then made 7,000 to 10,000 inquiries on names and Social Security numbers in the database and used some of those identities to commit at least $1 million worth of fraud. Assistant U.S. Attorney Mark Krause in Los Angeles said yesterday.”

35,000 California residents notified
Feb 8, 2005

ChoicePoint reveals problem not limited to California
Feb 16, 2005

38 state Attorneys-General demand notification
Feb 19, 2005

ChoicePoint states an additional 110,000 people affected
Feb 21, 2005

Final class action lawsuit settled for $10M
Jan 28, 2008

ChoicePoint suffers another breach
Oct 19, 2009

13,750 people exposed after a key data security tool failed for 4 months with no one noticing. FTC fines $275,000 and requires additional bi-monthly reporting.

“In April 2008, ChoicePoint, now a subsidiary of Equifax, Inc., turned off a key electronic security tool used to monitor access to one of its databases, and for five months failed to detect that the security tool was off, according to the FTC. During that period, an unknown person contacted unauthorized searches of a ChoicePoint database using sensitive consumer information, including Social Security numbers. The searches continued for 30 days. After discovering the breach, the company brought the name to the FTC’s attention.”
ChoicePoint suffers another breach
Oct 19, 2009

13,750 people exposed after a key data security tool disabled for 4 months with no one noticing. FTC fines $275,000 and requires additional bi-monthly reporting.

“In April 2008, ChoicePoint (now a subsidiary of Reed Elsevier, Inc.) turned off a key electronic security tool used to monitor access to one of its databases, and for four months failed to detect that the security tool was off, according to the FTC. During that period, an unknown person conducted unauthorized searches of a ChoicePoint database containing sensitive consumer information, including Social Security numbers. The searches continued for 30 days. After discovering the breach, the company brought the matter to the FTC’s attention.”
End of mandatory external security audits related to the 2004 breach.
Jan 1, 2026
End of mandatory external security audits related to the 2014 breach.
Jan 1, 2026
End of mandatory external security audits related to the 2004 breach.
Jan 1, 2026
### ChoicePoint Losses

<table>
<thead>
<tr>
<th>Category</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTC Settlement</td>
<td>$10M</td>
</tr>
<tr>
<td>Notification Costs</td>
<td>$2M</td>
</tr>
<tr>
<td>Legal and Professional Fees</td>
<td>$9.5M</td>
</tr>
<tr>
<td>Lost Sales From Business Practice Changes</td>
<td>$15M-$20M</td>
</tr>
<tr>
<td>Victim Trust Fund</td>
<td>$5M</td>
</tr>
<tr>
<td>Shareholder Lawsuit</td>
<td>$10M</td>
</tr>
</tbody>
</table>

Choicepoint: Unusual Activity Detected
Sep 27, 2004
Up to 310,000 people affected. "Multistate Anti-Terrorism Information Exchange" Fraud based on stolen IDs.
Bank of America

- On February 25th, 2005 reports surface that backup tapes with 1.2M credit card records are lost.
- The tapes contained information from a credit card program for federal workers, including 60 senators.
- Tapes believed stolen by baggage handlers in December.
- Sen. Pat Leahy, D-Vt holds Congressional hearing.
Up to 310,000 people affected. "Multistate Anti-Terrorism Information Exchange" Fraud based on stolen IDs.
CardSystems fails first PCI assessment
Jun 1, 2003
National Australia Bank first detects fraud.
Nov 1, 2004

Fraud traced to CardSystems Solutions
Jan 1, 2005

Visa and MasterCard begin investigations.
Apr 1, 2005

CardSystems states they discovered the breach and notified the FBI the next day.
May 22, 2005

Track 2 data stored and exposed.

MasterCard states CardSystems breached and 40 million transactions exposed.
Jun 17, 2005

Visa drops CardSystems
Jun 26, 2005

CardSystems acquired by Pay by Touch Solutions
Jul 18, 2005
National Australia Bank first detects fraud.
Nov 1, 2004

Fraud traced to CardSystems Solutions
Jan 1, 2005

Visa and MasterCard begin investigations.
Apr 1, 2005

CardSystems states they discovered the breach and notified the FBI the next day.
May 22, 2005

Track 2 data stored and exposed.

MasterCard states CardSystems breached and 45 million transactions exposed.
Jun 17, 2005

Visa drops CardSystems
Jun 30, 2005

CardSystems acquired by Pay by Touch Solutions
Oct 18, 2005
National Australia Bank first detects fraud. Nov 1, 2004

Fraud traced to CardSystems Solutions Jan 1, 2005

Visa and MasterCard begin investigations Apr 1, 2005

CardSystems states they discovered the breach and notified the FBI the next day. May 22, 2005

Track 2 data stored and exposed.

MasterCard states CardSystems breached and 40 million transactions exposed. Jun 17, 2005

Visa drops CardSystems Jun 30, 2005

CardSystems acquired by Pay by Touch Solutions Oct 18, 2005

Pay by Touch Pulls out Mar 30, 2006

Founder declared bankrupt in November/December. Firm appointed outside consultant warning company to shut down operations.
Nov 1, 2004

Fraud traced to CardSystems Solutions
Jan 1, 2005

Visa and MasterCard begin investigations.
Apr 1, 2005

CardSystems states they discovered the breach and notified the FBI the next day.
May 22, 2005

Track 2 data stored and exposed.

MasterCard states CardSystems breached and 40 million transactions exposed.
Jun 17, 2005

Visa drops CardSystems
Jun 30, 2005

CardSystems acquired by Pay by Touch Solutions
Oct 18, 2005

CardSystems PCI Certified
Jun 1, 2004

2005  2006  2007  2008  2009
Apr 1, 2005

CardSystems states they discovered the breach and notified the FBI the next day.
May 22, 2005

Track 2 data stored and exposed.

Jun 17, 2005

MasterCard states CardSystems breached and 40 million transactions exposed.

Jun 30, 2005

Visa drops CardSystems

Oct 18, 2005

CardSystems acquired by Pay by Touch Solutions

The Death of CardSystems
Pay by Touch Shut down.
Mar 19, 2008
Founder declared bankruptcy in November/December. Court appointed outside consultant to manage company, but later shut down operations.
Pay by Touch Shut down.
Mar 19, 2008
Founder declared bankruptcy in November/December. Court appointed outside consultant to manage company, but later shut down operations.
Lies, Damn Lies and Statistics
I used to think correlation implied causation.

Then I took a statistics class. Now I don't.

Sounds like the class helped. Well, maybe.
Special thanks to the Open Security Foundation, home of the DataLossDB
Consolidated Incidents by Type

- Lost/Stolen Media/Devices: 50%
- Hack/Web: 30%
- Fraud/Social Engineering: 8%
- Email: 4%
- Unknown: 4%

Legend:
- Lost/Stolen Media/Devices
- Hack/Web
- Fraud/Social Engineering
- Email
- Unknown
- SnailMail
Securosis 2010 Data Security Survey
Breaches Year Over Year

- Many more: 2%
- A few more: 10%
- About the same: 46%
- A few less: 12%
- Many less: 15%
- Other/NA/Don’t Know: 15%
### Major Incidents

<table>
<thead>
<tr>
<th></th>
<th>External</th>
<th>Internal</th>
<th>Accidental</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulated Data</td>
<td>193</td>
<td>221</td>
<td>266</td>
<td>680</td>
</tr>
<tr>
<td>Other PII</td>
<td>193</td>
<td>230</td>
<td>254</td>
<td>677</td>
</tr>
<tr>
<td>IP</td>
<td>137</td>
<td>164</td>
<td>167</td>
<td>468</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>523</strong></td>
<td><strong>615</strong></td>
<td><strong>687</strong></td>
<td><strong>1825</strong></td>
</tr>
</tbody>
</table>

### Minor Incidents

<table>
<thead>
<tr>
<th></th>
<th>External</th>
<th>Internal</th>
<th>Accidental</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulated Data</td>
<td>191</td>
<td>211</td>
<td>264</td>
<td>666</td>
</tr>
<tr>
<td>Other PII</td>
<td>225</td>
<td>265</td>
<td>312</td>
<td>802</td>
</tr>
<tr>
<td>IP</td>
<td>149</td>
<td>173</td>
<td>183</td>
<td>505</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>565</strong></td>
<td><strong>649</strong></td>
<td><strong>759</strong></td>
<td><strong>1973</strong></td>
</tr>
</tbody>
</table>
I know of no cases where lost/stolen media resulted in fraud.
Up to 310,000 people affected. "Multistate Anti-Terrorism Information Exchange" fraud based on stolen IDs.

Bank of America
May 23, 2005

CardSystems Solutions
Jun 17, 2005

Federal Deposit Insurance Corp.
Jun 17, 2005

Visa, MasterCard, American Express
Jun 19, 2005

Cleveland State University
Jun 4, 2005

Duke University Medical Center
Jun 4, 2005

University of Hawaii
Jun 17, 2005

University of Colorado at Boulder
Jul 21, 2005

Medix Health Plans
Jun 29, 2005
McAfee
Feb 23, 2006

Deloitte & Touche employee leaves a CD with personal records of 9,290 McAfee employees in airline seatback.
A KPMG International employee leaves a CD with personal data of 9,290 McAfee employees in airline seatback.
Chase Card Services
Sep 7, 2006

Florida National Guard
Sep 7, 2006

Liberty Mutual Insurance Co
Sep 7, 2005

Linden Lab, Second Life
Sep 8, 2006

Sentry Insurance (Accenture)
Jul 29, 2006
The Strange Life of Albert Gonzales

• During his senior year of high school, Albert Gonzales defaces government servers in India from his high school library.
• The FBI responds, confiscates two computers.
• Gonzales told to stay away from computers for 6 months, but otherwise off the hook.
• After graduation, he moves to NYC, then Kearny, N.J.
• In NJ, Gonzales becomes the leader behind the ShadowCrew site.
• Gonzales arrested by federal agents in 2003 for possession of 15 fake credit and debit cards.
• “CumbaJohnny” becomes a Secret Service informant for “Operation Firewall”, leading to the arrest of 28 ShadowCrew members in 2004 accused of stealing 1.5M credit card accounts.
• Authorities believe $4.3M stolen by ShadowCrew members.
• Gonzales moves back to Miami and founds a computer consulting service.
• While in Miami, Gonzales starts *Operation Get Rich or Die Tryin’*, earning at least $1.6M.
Round 1
TJX

• On December 18th, 2006, TJX discovers suspicious software on their systems.

• The Secret Service begins investigating, and banks, credit card processors, and credit card companies are notified the day after Christmas.

• The breach becomes public on January 17th, 2007.
45.7 Million Customers Initially Affected
• TJX charged off $5M in the first 3 months after the breach for investigation and remediation.

• By August, estimated losses rose to $256M.

• Sales rose 9% over the same period the previous year, to $4.3B in the second quarter.

• The breach went back to at least 2005.
Banks are currently seeking class action status for a lawsuit to recover costs of fraud and re-issuing credit cards.

In a court filing, fraud related charges for Visa alone range from $68M to $83M.

Visa has fraud reports in 13 countries.
Based on the class action court filings.

94 Million Records Exposed
• Breach via WEP hacking along US1 in Miami.
• Sniffer programmed by a former Morgan Stanley employee grabbed card numbers.
• Breach began in July, 2005.
• Also breached BJ’s Wholesale Club, Boston Market, Forever 21, OfficeMax, Sports Authority, and DSW.
Round 2
• From April to September, 2007, Gonzales and friends install sniffers on point of sale terminals at Dave and Buster’s.

• At least $600,000 in fraudulent transactions from 675 cards taken from one store.

• Gonzalez arrested in May 7, 2008.
Round 3
Later revealed that Target and J.C. Penney were the undisclosed breaches who fought to remain confidential.
February, 2009- Visa and FBI release alert with details of the attack methods (Gonzales not specified).
They identify Web sites that are vulnerable to SQL injection. They appear to target MSSQL only.

They use "xp_cmdshell", an extended procedure installed by default on MSSQL, to download their hacker tools to the compromised MSSQL server.

They obtain valid Windows credentials by using fgdump or a similar tool.

They install network "sniffers" to identify card data and systems involved in processing credit card transactions.

They install backdoors that "beacon" periodically to their command and control servers, allowing surreptitious access to the compromised networks.

They target databases, Hardware Security Modules (HSMs), and processing applications in an effort to obtain credit card data or brute-force ATM PINs.

They use WinRAR to compress the information they pilfer from the compromised networks.
At Heartland, it was the compromise of a non-transaction system then leveraged to hit the transaction network during a VPN connection.
Gonzales and friends would identify potential targets, then use a combination of online and physical surveillance to identify weaknesses. Physical visits would reveal the payment system being used (via the point of sale terminals), and other relevant information. When performing online reconnaissance, they would also attempt to determine the payment processor/processing system.
Eli Lilly leak to the New York Times revealed
Feb 5, 2008

Entire case file accidentally emailed to Alex Berenson instead of Bradford Berenson

Cornell University
Mar 4, 2008

Hannibal
Mar 17, 2008

Chinese Ministry of Education
May 11, 2008

Dave & Busters

Rhode Island Department of Administration
Mar 21, 2008

BNY Mellon Shareowner Services
Mar 28, 2008

University of Miami
Apr 17, 2008

Sungard
May 12, 2008

University of Oregon Health & Science
Jul 14, 2008

Outpost Internets
Apr 10

"All the news
That's fit to print"

-Lilly
Countrywide Home Loans
Aug 1, 2008

The data theft, originally attributed to a single employee working over a two-year-period, exposed tens of thousands of customer records.

In Apr, 2010 16 plaintiffs seek $20M in a class action lawsuit due to Countrywide’s poor handling of the breach.
RBS WorldPay

- Hack occurred on November 10, 2008.
- Up to 1.5M records compromised.
- Over $9M in cash stolen via ATM.
RBS WorldPay

- First attacker identified vulnerability in RBS network in November and contacted associates.

- Username and password given to second attacker, who gained access to a database of ATM account numbers and PINs.

- Reverse engineered PIN codes.

- Limits and withdrawal limits on 44 pre-paid payroll cards raised in the database.
Three days later, on November 8, over 2100 ATMs in at least 280 cities used in a 12 hour spree.

Attackers monitored and covered tracks in real time.

Money mules kept from 30-50% of their individual take. Access tracked in real time by core attackers.

RBS officials quickly identified the attack and notified authorities.
• Logs not completely erased, leaving evidence for investigators.

• “The early detection of fraudulent ATM withdrawal activities in Tallinn, Estonia led to an immediate response by the Estonian Central Criminal Police. Their investigative efforts led to the prompt identification of TŠURIKOV, GRUDIJEV, the TSOIs, and JEVGENOV. TŠURIKOV is presently in custody in Estonia on charges related to access device fraud. The extradition of TŠURIKOV to the United States is currently in process. Access device fraud charges are also pending in Estonia against GRUDIJEV, the TSOI’s, and JEVGENOV. Cooperation between the Hong Kong Police Force and the FBI also led to a parallel investigation, resulting in the identification and arrest of two individuals who were responsible for withdrawing RBS WorldPay funds from ATM terminals in Hong Kong. The Netherlands Police Agency National Crime Squad High Tech Crime Unit and the Netherlands National Prosecutor’s Office provided key assistance in the investigation.” -FBI release
• Attackers indicted by a federal Grand Jury in Atlanta on November 10, 2009.

• “Five of the defendants, Igor Grudijev, Ronald Tsoi, Evelin Tsoi, Mihhail Jevgenov and Sergei Tsurikov are being held in Estonia. Tsurikov is awaiting extradition to the U.S., while the other four are to be prosecuted in Estonia. The other defendants are Viktor Pleshchuk of St. Petersburg, Russia, Oleg Covelin of Chisinau, Moldova, and a person the prosecutors identified only as "Hacker3."” -Threatpost
The Non-Disclosure

- Client A disclosed a data breach.
- The breach was at their processor/hoster, not in their systems.
- Client A knows that 4-5 competitors were also exposed in the same incident.
- None of them disclosed.
WSJ reports F-35 plans stolen from Lockheed
Apr 20, 2009

Later reports indicate no classified information lost, but maintenance materials.
Google threatens to leave China after massive attack.
Jan 12, 2010

Attack of the APT!!!
Albert Gonzales sentenced to 20 years in Federal Prison
Mar 25, 2010

He would forfeit more than $1.65 million, a condominium in Miami, a blue 2006 BMW 330i automobile, IBM and Toshiba laptop computers, a Glock 27 firearm, a Nokia cell phone, a Tiffany diamond ring and three Rolex watches.
Lifting the Veils
Key Findings

- Companies don’t usually notice their breaches—they are discovered by a 3rd party (91% Trustwave, 61% Verizon).
- Most attacks in both reports not considered highly difficult (85% Verizon).
- SQL Injection, application attacks, remote access, and malware are the top vectors.
Key Findings

• Partners represent a high risk vector (both orgs use different definitions, but numbers are over 80%).

• Mistakes play a massive role (67% Verizon).

• Memory parsing malware on the rise.
### Verizon/USSS

- 70% resulted from external agents
- 48% were caused by insiders
- 11% implicated business partners
- 40% resulted from hacking
- 38% utilized malware (<>)
- 28% employed social tactics
- 15% used physical attacks
Disclosure Eras

- **Bad Luck and Trouble** (2005)
- **Land of the Lost** (2006)
- **Gonzales** (2007)
What Our Clients Tell Us

- Data protection is misaligned- for example, most clients use DLP on email first or only.
- Internal politics and lack of management are nearly insurmountable.
- Concern over IP loss is growing (uptick in DRM calls).
- Compliance is the biggest driver.
Personal Security Guiding Principles

• Don't expect human behavior to change. Ever.

• Not all threats are equal, and all checklists are wrong.

• You cannot eliminate all vulnerabilities.

• Surprise is your enemy.

• You will be breached.
React faster and better. Incident response is more important than any other single security control.
Involuntary Case Studies in Data Breaches

Mike Rothman
securosis.com/blog
mrothman@securosis.com
@securosis @securityincite