Should Credit Card Issuers Reissue Cards After a Data Breach?

Jim Graves, Alessandro Acquisti, Nicolas Christin
Carnegie Mellon University
Issuer Options Post-Breach

• When a credit card is compromised in a breach, issuers can recover “fraud losses” from an merchant’s acquiring bank but not “operational costs.”

• The law expects plaintiffs to mitigate damages

• Issuer choices:
  • Reissue all cards; possibly without reimbursement
  • Wait and see; may not have mitigated damages
Research Question

• Which option has the lowest societal cost?
Challenges

• Poor data
  • What is the likelihood that a card affected in a breach will be used for fraud?
  • How many credit cards are affected in breaches?
  • How much credit card fraud is due to breach?
Research Approach

• Cost-benefit estimation
• Ranges
• Monte Carlo analysis
• Focused primarily on direct costs
Cost of Reissuing Cards

- $3–$25
- Based on claims in lawsuits and figures quoted in news articles
- Economies of scale seem to apply

<table>
<thead>
<tr>
<th>Source</th>
<th>Cards</th>
<th>Cards $/Card</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pa. State Empl. Credit Union 1</td>
<td>20,000</td>
<td>$5</td>
</tr>
<tr>
<td>Fulton Bank 2</td>
<td>20,000</td>
<td>$5</td>
</tr>
<tr>
<td>Sovereign Bank 3</td>
<td>81,000</td>
<td>$6</td>
</tr>
<tr>
<td>Merrill Bank 4</td>
<td>71</td>
<td>$14</td>
</tr>
<tr>
<td>TrustCo Bank 5</td>
<td>4,000</td>
<td>$20</td>
</tr>
</tbody>
</table>

2 Eric Stark, Computer Hackers are Stealing Bank Card Information, but There Is Protection and Some Banks Have Been Aggressive, Sunday News (Lancaster, Pa.), July 11, 2004, at 1
3 Mark Jewell, IDs Are a Steal, Columbian (Vancouver, WA), Aug. 23, 2004, at E
Cost of Not Reissuing Cards

• Expected cost of fraudulent use
• Cost of fraud
• Probability of misuse
• Easy to calculate with the right data
• We do not have the right data
• But maybe we can estimate with data we have?
Estimating the Cost of Not Reissuing Cards

- Can estimate based on
  - Number of credit card accounts breached (and not reissued) per year
  - Number of credit card fraud incidents per year
  - Percentage of those incidents in which card information was obtained via breach
Estimating the Cost of Not Reissuing Cards

- These data sources also have problems!
- (But at least the data exist.)
Data Issues

• Cards vs. accounts vs. households
• How many breached credit card accounts?
• How much card fraud is because of breach?
• How effective is fraud monitoring at reducing fraud?
Cards, Accounts, or Households

- Cards per account: ~1.2; accounts per household: ~6–9
How Many Breached Credit Cards?

- Disclosed breaches
- Known but undisclosed breaches
- Undetected breaches
Estimating the Number of Breached Credit Cards

• Manually extracted from PRC database breaches affecting credit cards
• Ranges for disclosed breaches with record counts
• Extrapolation to disclosed breaches without record counts
  • Weighted by breach type (hack, lost media, etc.)
**Estimated Number of Cards Exposed in Breaches per Year (000s)**

<table>
<thead>
<tr>
<th>Description</th>
<th>Low</th>
<th>Point</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reported w/ record counts</td>
<td>35,000</td>
<td>38,000</td>
<td>41,000</td>
</tr>
<tr>
<td>Credit cards as percentage of breached payment cards</td>
<td>66%</td>
<td>72%</td>
<td>78%</td>
</tr>
<tr>
<td>Credit card numbers reported lost in breaches per year</td>
<td>23,100</td>
<td>27,400</td>
<td>32,000</td>
</tr>
<tr>
<td>Est. records per year in breaches with unknown record counts</td>
<td>150</td>
<td>2,900</td>
<td>7,500</td>
</tr>
<tr>
<td>Scaling factor for unreported or undetected breaches</td>
<td>1</td>
<td>1.34</td>
<td>2</td>
</tr>
<tr>
<td>Portion of breached cards reissued</td>
<td>0.90</td>
<td>0.78</td>
<td>0.60</td>
</tr>
<tr>
<td>Total</td>
<td>2,460</td>
<td>12,000</td>
<td>40,600</td>
</tr>
</tbody>
</table>
How Much Credit Card Fraud is Because of Breach?

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Javelin</td>
<td>65%</td>
<td>54%</td>
<td>13%</td>
<td>56%</td>
<td>47%</td>
<td>64%</td>
</tr>
<tr>
<td>ITRC</td>
<td>4%</td>
<td>3%</td>
<td>5%</td>
<td>27%</td>
<td>4%</td>
<td></td>
</tr>
<tr>
<td>FTC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIMIP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BJS*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* Existing-account credit card fraud only

Legend:
- Other
- Stolen from mail
- Knew thief
- Lost/stolen from wallet, home, car, etc.
- Phish/hack/Internet
- Transaction/scam/skimmer etc.
- Breach/company controlled
- Unknown
How Effective is Fraud Monitoring at Reducing Fraud?
## Expected Per-Card Cost of Not Reissuing Credit Cards

<table>
<thead>
<tr>
<th>Description</th>
<th>Low</th>
<th>Point</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P(EACCF \mid \text{breach}) (\rho_{k,0})$</td>
<td>0.0005</td>
<td>0.0056</td>
<td>0.0605</td>
</tr>
<tr>
<td>Cost of EACCF ($f_{k,0}$)</td>
<td>$1,000</td>
<td>$1,366</td>
<td>$1,500</td>
</tr>
<tr>
<td>Fraud reduction from flagging exposed cards</td>
<td>0%</td>
<td>10%</td>
<td>20%</td>
</tr>
<tr>
<td>Expected cost per card of not reissuing</td>
<td>$0.41</td>
<td>$7.50</td>
<td>$109.00</td>
</tr>
</tbody>
</table>
Monte Carlo Analysis of Results
Per-Card Costs

![Cost distribution graph](image)

- **Cost of not reissuing**
- **Cost of reissuing**

**Relative Frequency**

**Cost per Card**

Costs range from $0 to $70 with relative frequencies ranging from 0 to 0.3.
Total Cost Savings by Not Reissuing

Cumulative Savings (millions)

X ≤ -790
5%

X ≤ 0
26.3%

X ≤ 420
95%

Mean: $9.5 million
Median: $132 million
Mode: $100 million

P(Cumul. Savings) in 10^-6

-2500 -2000 -1500 -1000 -500 0 500 1000

Mean: $9.5 million
Median: $132 million
Mode: $100 million
Correlation Coefficients

- Mean fin. cost of existing-account card fraud: 0.73
- % of existing-account card fraud from breach: 0.21
- % of breached cards reissued: 0.18
- Reported but unknown breached records per year: -0.09
- Unreported breach scaling factor: -0.08
- Credit card accounts per household: -0.06
- Households victimized: 0.04
- Fraud reduction from flagging breached cards: -0.03
- Hours spent responding to existing-account card fraud: 0.03
## Where to Improve Data?

<table>
<thead>
<tr>
<th>Data</th>
<th>How to Address it?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percent of fraud resulting from breach</td>
<td>More study</td>
</tr>
<tr>
<td>Effectiveness of fraud monitoring</td>
<td>Issuer disclosure?</td>
</tr>
<tr>
<td>Number of undetected and undisclosed breaches</td>
<td>Incentives to detect and disclose?</td>
</tr>
</tbody>
</table>
Conclusions

• Reissuing cards immediately after a breach may be *more* expensive than waiting until fraud is attempted.

• But this depends greatly on data that needs improvement.
Questions?