Mitigating Reputational Risk & Restoring Customer Trust:
Optimizing the Role of PR In Data Breach Response

Brian Lapidus, Practice Leader, Identity Theft & Breach Notification, Kroll
Zach Olsen, President, Infinite Global
Kelsey Eidbo, Client Supervisor, Infinite Global
It’s rough out there…

22 Million
PII
2012 - 2014
Security clearance
information part of the breach

110 Million
Credit cards
2013
$162 Million
estimated cost of the breach

3 Billion
User accounts
2013-2014
$350 Million
est. decrease in sale price to Verizon

145 Million
User accounts
2014
Days: 229
hackers had access to internal data

83 Million
Contact Information
2014
$250 Million
spent on security annually

143 Million
PII
2017
2+ months
est. time to discover the breach

SOURCE: The 16 biggest data breaches of the 21st century, CSO, October 11, 2017
And the incident is just the beginning...

- Remediaion
- Business disruption
- Customer churn
- Finances
- Legal costs
- Brand reputation
- Financial loss
- Notification costs
- Ongoing monitoring
... but a strong communications plan can help here:
... and potentially here:

- Remedia**tion**
- **Business Disruption**
- Customer Churn
- **Brand Reputation**
- **Financial Loss**
- **Legal Costs**
- **Notification Costs**
- **Ongoing Monitoring**
Data Breaches Can Cause Customer Churn

Figure 1: Avoidance of Further Business, by Type of Organization in Which Data Breach Occurred

- **Merchant**
  - Strongly Disagree: 13%
  - Somewhat Disagree: 23%
  - Neutral: 32%
  - Somewhat Agree: 18%
  - Strongly Agree: 15%

- **Healthcare provider**
  - Strongly Disagree: 16%
  - Somewhat Disagree: 15%
  - Neutral: 39%
  - Somewhat Agree: 19%
  - Strongly Agree: 11%

- **Financial institution or credit card issuer**
  - Strongly Disagree: 19%
  - Somewhat Disagree: 23%
  - Neutral: 34%
  - Somewhat Agree: 15%
  - Strongly Agree: 9%

Q2D. Please indicate the type of organization where the data breach occurred. Please read each of the following statements carefully and indicate your level of agreement (*I avoid doing further business with the organization(s)*) shown.

October 2013, n = varies: 111 – 897

Base: All consumers whose PII was breached at an FI or CC issuer,
All consumers whose PII was breached at a merchant,
All consumers whose PII was breached at a healthcare provider
Crisis communications is part of a defensible security strategy
Pre-breach Communications Planning

- Find an experienced outside public relations team, get to know them ahead of an incident, and introduce them to your in-house response team.

- Develop a crisis communications playbook that covers (at minimum):
  - The crisis communications team and contact information for all members (in-house and external)
  - Internal and external audiences
  - Media policies to be distributed firm-wide before an incident and on a regular basis.
  - Contact information of key journalists

- Run a tabletop exercise with all crisis communications team members

- Keep your plan, and the people involved, fresh
Responding to a Breach: The Role of PR

A good PR firm will help an organization:

▪ Understand the media landscape that is specific to them and their industry
▪ The media cycle of a data breach
▪ How to communicate to critical audiences throughout a breach
▪ When and how to leverage social media
▪ Managing the expectations of “interested” vs. “affected” parties
▪ Maintain consistency of messaging when communicating across various platforms
▪ When to be proactive, reactive or quiet
Responding to a Breach: The Role of PR – cont’d

A good PR firm will help an organization:

- Anticipate the next phase of the news cycle, and advise on how to plan and react
- Determine “best case” and “worst case” scenarios provide counsel on how to proactively address internal questions
- Control the pace with which media is responded to
- Liaise between legal team and client to ensure all communications – internal and external – are meeting the needs and goals of all parties
CUSTOMIZED, COMPLIANT COMMUNICATIONS

- When/Where did the theft/breach occur?
- What happened? What was lost or stolen?
- What is [CLIENT] doing about this?
  [SAMPLE: Client immediately notified local law enforcement and is cooperating with them as they continue their investigation.]
- What is [CLIENT] doing to prevent this from happening in the future?
  [SAMPLE: [CLIENT] has examined and analyzed existing procedures and systems to ensure appropriate security measures are (reinforced/in place).]
- Why wasn’t I notified sooner?
  [SAMPLE: [CLIENT] immediately notified local law enforcement officials and launched an investigation into the incident. The investigation included a review of internal security systems to confirm that procedures already in place are strengthened to further safeguard against a breach of data security in the future. Last, it was imperative that impacted individuals were identified and their contact information gathered into a consistent format for notification. This investigation was a time-consuming process, but Client believed it was necessary to ensure appropriate precautions and next steps were taken.]
How it Works – Breach Notification

- Distill the data for optimized mail delivery
  - Standardize addresses, report and remedy exceptions
  - Sort and group special populations
  - Compare against NCOA database
  - Dedicate a toll-free telephone number; include in notice

- Draft notification letter(s) congruent with state law(s) and audience(s)
  - Include clear guidelines about how to use any services offered to help mitigate identity theft fears and threats

- Monitor and report on returned mail
Consider: Proof that Stands Up Later

Case Studies

- Case #1: Rapid, Large-scale Response
  - Onsite implementation, ready to be on ground in 48 hours,
  - Multiple letter versions
  - Banner on Kroll.com homepage to steer people to public notice page

- Case #2: Supporting clients in litigation following an event
  - Supplied post-event reporting, documentation, and recorded calls
  - Provided onsite deposition and case preparation data to help demonstrate the expertise of the services provided to notification subjects
Q&A

Contact Details

Brian Lapidus  
Practice Leader  
Identity Theft and Breach Notification  
T +1 615.577.6770  
blapidus@kroll.com

Kelsey Eidbo  
Client Supervisor  
T +1 415.732.7804  
kelseye@infiniteglobal.com

Zach Olsen  
President  
T +1 415.732.7802  
zach@infiniteglobal.com