Not All Breaches Are Created Equal

Nicholas L. Cramer
Director of Data Breach Response
Agenda

• Understanding The New Role of Cyber Insurance

• 1st Party Risk vs. 3rd Party Risk

• The “Go-Live” Timeline

• Interpreting The Risk of Harm

• Remediation Through Identity Protection

• Proving The Extent of Harm

• Applying Lessons learned
About the Speaker

• Joined Debix in 2008, previously developed and sold Enterprise Resource Planning (ERP) technology to mid-size Consumer Reporting Agencies

• Managed the response for over 1200 data breach events
  – Single four largest Healthcare breaches since HITECH
  – Single largest breach in U.S. history requiring ID Protection

• Designed and developed proprietary “go-live” methodology on the force.com platform
  – Over 50,000,000 consumers notified since 2008
What Do You Mean, All Breaches Are Not Created Equal?

A wise privacy professional once said, “all breaches are not created equal”. It merely takes involvement in that second breach event to truly appreciate the rightfulness of this statement.

In this session, we’ll take an outspoken look, from an insider’s perspective, at the operational, logistical, cost and value considerations in responding to data breaches of all sizes.

Whether you’re considering an in-house response, or partnering with one or more vendors, we’ll address some of the most common misconceptions and key questions in a successful response.

A Quick Clarifying Point...

The content in which we will be discussing in this session is purely around the “response” components involved once a decision has been made to notify.
Data Breaches: A Significant Risk That Requires Preparation

Business Risk

- **Regulators** Require Rapid Response
- **$202** Average Cost per Record Lost
- **Tarnishes** Existing Brand
- **Drives** Customer Churn

Business Risk

- 8X Higher Fraud Victimization Rate Among Data Breach Victims
- 84% of Customers Impacted Experienced Increased Anxiety or Concern
- 75% of Customers Remember the Breached Brand

Of Impacted Customers Feel The Breached Organization Could Have Done More 68%

A Pervasive, Expensive Problem

1 in 5 U.S. Households Violated

542 Million Records Breached Since 2005

8.1 Million Fraud Victims Annually

Sources: Ponemon Institute, Javelin Research, AllClear ID Annual Consumer Survey, Privacy Rights Clearinghouse, Carnegie Mellon & Temple University Study
A whole new set of insurance products are being developed/offered

- 1\textsuperscript{st} party claims = Breach response and remediation
- 3\textsuperscript{rd} party claims = Lawsuits from other businesses or individuals (class actions)

Either as an “endorsement” to an existing policy or a “standalone” policy usually labeled “media and technology”, “network security and privacy” or “cyber”.

There are ~50 insurance carriers who offer this coverage now

- there were 5 only five years ago.
Preparation Expedites The “Go-Live” Timeline

Data Breach → Decision To Notify → Notifications Begin Mailing → Call Center Accepting Calls → Enrollment Into ID Protection
Interpreting The Risk of Harm

Types of ID Theft:

- Employment ID Theft
- Medical ID Theft
- Criminal ID Theft
- Financial ID Theft
- Social Engineering

Know How To Remediate Each Type of Harm
Remediating Risk of Harm With Identity Protection

Credit Bureaus

Identity Monitoring

Medical

Cyber

Non-Credit

Geared for Early Detection and Possible Prevention
Remediating Risk of Harm With Identity Protection

• If Consumer is Victimized: Fraud Assistance
  – Restoration
  – Remediation
  – Recovery
  – Repair

• If Consumer is Liable for Fraud: ID Theft Insurance
  – $10,000
  – $25,000
  – $1,000,000

• If No Other Protections are Made Available: FCRA
  – $10,000
  – $25,000
  – $1,000,000
Now that we’ve appropriately addressed the risk of harm, how do I justify my analysis to…

– …regulators?
– …customers?
– …company stakeholders?
– …law enforcement?
– …the media?
Establish a clear two-way communication channel with an escalation protocol
Proving The Extent of Harm - QA

QA – The Right Way

- Time Spent on Quality Assurance
  - Call Close and Documentation
  - Escalation Procedures
  - How to Handle Existing Fraud
  - How to Leverage FCRA
  - Product Related Inquires/Phone Registration
  - Breach Related Inquires
Proving the Extent of Harm – Connecting The Dots

1. Establish Channel For Communication
2. Document Fraud (Suspected & Confirmed)
3. Look for Patterns & Correlations
4. Contact Law Enforcement

Pre “Go-live”  Post “Go-live”
Applying Lessons Learned

• IRD & Vendor closeout meetings
• Leftover materials
• Cost Analysis
• Compile & evaluate all test records
• Realized vs. Projected risk
• Share “war stories”
Thank You Very Much!

Questions?

nicholas.cramer@allclearid.com
www.allclearid.com