Data Breach Preparedness
Best Practices

FRAUD MITIGATION CHECKLIST

Created By: Ann Davidson, Vice President of Risk Consulting
Allied Solutions, LLC
Last Updated: August 2017
It’s not a matter of IF. It is a matter of WHEN a data breach will strike. Compliance with GLBA Section 401(b) requires that you have an Emergency Data Breach Response Plan in place and that it be exercised annually. Follow this quick checklist to determine how well prepared you are to deal with data breach.

**PLAN… WHILE YOU STILL CAN**

- Establish a written Data Breach Response Plan
  - Name your Data Breach Response Team
  - Perform Risk Assessments to determine your vulnerability and identify risks
  - Establish your Response Protocols, with timelines and responsibilities
  - Review your plan each year, and update with new solutions and new risks
  - Submit changes to your Board of Directors (GLBA) annually

- Conduct annual Data Breach Awareness Training for employees

- Run Tabletop Exercises and/or Mock Data Breach Drills annually

- Create a “Security Fund” for unpredictable external and internal breach costs

- Consider the benefits of giving identity protection services to your accountholders proactively to
  - Eliminate costs of internal breach later
  - Provide market differentiation
  - Generate revenue to contribute to your Security Fund
  - Offset many of the negative effects of external data breach, such as a retailer cc breach
  - Give your accountholders the best chance to defend against identity theft – where ever and whenever it may strike

**RESPOND… TO INTERNAL DATA BREACH**

- Activate your Data Breach Response Plan, including notification of law enforcement and regulators

- Designate internal or external resource to create an Action Plan

- Select internal or external resource to:
  - Draft notification letters
  - Distribute employee scripts
  - Create FAQs for website
  - Write press releases and other PR

- Contract with external resources to provide printing and mailing services for notification letters

- Contract with external resources to provide specialized legal assistance, if necessary. This specialized legal service will also be able to contract for forensic investigative services, if necessary.

- Stage your mailing for letters to arrive early in the week
RECOVER... YOUR BRAND AND PROTECT YOUR ORGANIZATION

✓ Designate resources that will provide professional breach customer support services (this may be same group that performs identity investigation and remediation services below)
  ◦ Answering questions about fraud and identity theft
  ◦ Assisting with credit and other monitoring services enrollment
  ◦ Assisting with placement of fraud alerts

✓ Designate resources that will provide professional identity fraud investigation and fraud remediation services to offset consumer “damages”
  ◦ Performing professional investigation to determine extent of fraud damage
  ◦ Remediation fraudulent transactions on behalf of affected consumer using LPOA
  ◦ Performing recovery steps by expunging fraudulent data from credit reports and other data sources to clean up consumer’s identity
  ◦ DO NOT TRUST THESE TASKS TO A CALL CENTER. The minimum requirement for a professional Identity Recovery Advocate is FCRA/FACTA certification, HIPAA certification, and a license for private investigator. Other certificates, such as CITRMS are not by themselves enough to justify a professional investigator
  ◦ Make sure that ALL individuals who will be serving your consumers are appropriately certified, licensed and trained

✓ Designate resources that will provide credit/other monitoring services to be provided at no-cost for consumers
  ◦ Contract in advance for these services to lock-in rates and avoid costly implementation fees
  ◦ Give-away monitoring services in advance of a breach to save on expense, recapture cost and to create more value in your account relationships
  ◦ Make sure that the vendor has no cross-selling privileges unless you have contracted for these services, at time of breach and after the term of service expires
  ◦ Test the activation process. Can the consumer activate all of the services in one registration process? Do not subject the consumer to multiple steps to register.

✓ Evaluate response effectiveness and modify Data Breach Response Plan accordingly
  ◦ Where were critical errors made in following the plan’s procedures?
  ◦ Where did the procedures come up short in providing the direction that the team needed?
  ◦ What steps/issues could have been avoided with proper pre-planning or different procedures?
  ◦ Re-evaluate the assignments of the Data Breach Response Team. Are any changes warranted?
  ◦ Make any necessary changes and submit changes to the Board of Directors
  ◦ Implement new policies, procedures and employee training properly to engage new processes

For more information, contact Melissa Eldredge, Marketing, Sales, and Public Relations Liaison for Allied Solutions, at melissa.eldredge@alliedsolutions.net.