



# **Online Lead Generation: Data Security Best Practices**

**Released September 2009**

**The IAB Online Lead Generation Committee has developed these Best Practices.**

**About the IAB Online Lead Generation Committee:**

The mission of the IAB Lead Generation Committee is to define best practices that ensure lead quality and improve conversion, and to educate marketers and agencies on lead generation/customer acquisition as a cost-effective vehicle for advertisers to gain high quality customers. The committee will also evangelize lead generation targeting to new industries not utilizing lead generation today. A full list of Committee member companies can be found at:

[http://www.iab.net/member\\_center/councils\\_committees\\_working\\_groups/committees/lead\\_generation\\_committee](http://www.iab.net/member_center/councils_committees_working_groups/committees/lead_generation_committee)

This document can be found on the IAB website at:

[http://iab.net/data\\_security](http://iab.net/data_security)

IAB Contact Information:

Gina Kim

Director of Industry Services, IAB

212-380-4728

[Gina.Kim@iab.net](mailto:Gina.Kim@iab.net)

## **Table of Contents**

---

Executive Summary .....	3
Data Security History .....	6
Data Storage & Retention.....	7
Market Regulations .....	10
Network Controls .....	14

## Executive Summary

---

The IAB Data Security Best Practices provide best practices to advertisers and publishers for the storage of online lead generation data in a secure format, where the safety and integrity of consumers' personally identifiable information<sup>1</sup> (PII) is assured. The benefit of following these best practices is to ensure that consumer data is stored securely to prevent security vulnerabilities, threats and fraud.

These best practices were developed by interviewing several leading online lead generation companies across major verticals, including education, CPG, retail, insurance, real estate, catalog/continuity, and healthcare. These companies were asked to describe their data storage, retention, and security methods, how they consider various market regulations in their data security practices, and what their network controls and policies are for data security monitoring and auditing.

The recommendations outlined in this document address three areas:

1. Data Storage & Retention
2. Market Regulations
3. Network Controls

Key Best Practices include:

- Advertisers and publishers should have an up-to-date written data retention, disposal policy and procedure document
- Advertisers and publishers should consider market regulations specific to their industry
- User access to consumer data should be restricted and enforced with technical security measures
- Data security responsibility should be incorporated into an internal job function

### **Definition: Data Security for Online Lead Generation**

Data security for online lead generation is defined as the secure storage, maintenance and audit of consumer PII and other consumer data upon submission of a lead generation form on a publisher website.

### **Definition: Online Lead Generation Offers on a Publisher Website**

While registering on a publisher website, the consumer is presented with lead generation offers from third party advertisers. Consumers may select offers of interest, fill out a form(s) providing additional PII, and give consent to share their PII with the advertiser or third parties. In exchange, the consumer receives information or services from the advertiser (e.g. free quote, newsletter, or coupon).

---

<sup>1</sup> According to the IAB, PII means information that can be used to identify, contact or locate a consumer and refers to information such as an individual's first and last name coupled with, mailing address, phone number or e-mail address.

Publishers generally offer two types of online lead generation to advertisers: 1) Simple offers where the consumer may sign up for the offer without entering additional information, and 2) Custom offers where the consumer is required to enter additional information in order to sign up for the offer.

Another form of online lead generation is a specific website designed to capture leads, such as automotive or education sites, where a form is presented to consumers giving consent to share their PII with that advertiser and/or other third party advertisers.

In both cases, the PII provided by consumers may be as simple as first name, last name and email address. Additional contact information may also be collected such as physical address, phone number, and credit card number.

With the completion of Data Security Best Practices, the full life cycle of online lead generation best practices has been documented and published by the IAB Lead Generation Committee:

Before an online lead generation offer goes live, advertisers and publishers should consider these best practices to ensure high quality leads are generated and the regulatory environment is considered:

1. **The Marketer and Agency Guide to Lead Generation.** Published in March 2007, this document helps marketers and agencies understand how to assess the overall quality of leads generated online by defining and addressing the key aspects of lead quality. Key aspects of lead quality include: lead origination, consumer motivation, lead exclusivity, lead age, and verification of data fields.

[http://www.iab.net/media/file/LeadQualityWhitePaper\\_031607-1.pdf](http://www.iab.net/media/file/LeadQualityWhitePaper_031607-1.pdf)

2. **B2B and B2C Best Practices for U.S.-based Advertisers and Publishers.** Published in February 2008, the document provides organizations with principles of good conduct by defining best practices and educating advertisers and publishers on implementation of those best practices. Best practices include: consumer disclosures, privacy policies, data ownership, usage, and sharing.

<http://www.iab.net/media/file/B2CandB2BBestPracticesFINALv3.pdf>

After the lead is submitted, consumer data should be transferred securely from the advertiser to the publisher:

3. **Lead Generation Data Transfer Best Practices.** Published in August 2007, this document standardized the transfer and receipt of data between advertisers and publishers in order to safeguard consumer data and create operational efficiencies. Best practices include: proper encryption formats, standard formats, and set up of data feeds.

[http://www.iab.net/media/file/standards\\_pdf\\_LeadGenerationDataTransferBestPractices.pdf](http://www.iab.net/media/file/standards_pdf_LeadGenerationDataTransferBestPractices.pdf)

After leads are submitted and transferred securely, consumer data should be stored securely by advertisers and publishers:

4. **Online Lead Generation: Data Security Best Practices.** Published in September 2009, this document provides best practices to advertisers and publishers for the storage of online lead generation data in a secure format. Best practices include: data storage and retention, market regulations, and network controls.

[http://www.iab.net/data\\_security](http://www.iab.net/data_security)

As leads are generated, advertisers and publishers should work together to optimize campaigns to improve ROI:

5. **Lead Quality Accountability Best Practices for Advertisers and Publishers.** Published in December 2008, the document defines 1) best practices for the advertiser sharing of invalid leads with publishers to optimize campaigns and 2) best practices for the advertiser sharing of converted leads with publishers to improve advertiser conversion quality. Best practices include: defining lead quality, invalid lead reason code inclusion, and publisher usage of invalid and converted lead data.

<http://www.iab.net/media/file/leadqualitybp.pdf>

## Data Security History

---

Over the past quarter century, the United States government has studied the manner in which entities collect and use personal information – their "information practices" – and the safeguards required to assure those practices are fair and provide adequate privacy protection. The result has been a series of reports, guidelines, and model codes that represent widely-accepted principles concerning fair information practices. Common to all of these documents [hereinafter referred to as "fair information practice codes"] are five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.<sup>2</sup>

Over time, the Federal Trade Commission (FTC) has developed a generally applicable data security standard, consistent with existing laws and the FTC's many enforcement actions, which requires companies to implement "reasonable" data security practices. The protections should be based on the sensitivity of the data being collected, the nature of a company's business operations, the types of risks a company faces, and the reasonable protections available to a company.

In addition, the FTC has come out with PROTECTING PERSONAL INFORMATION - A Guide for Business that provides an excellent framework for getting started. The following steps have been extracted from the guide.

A sound data security plan is built on 5 key principles:

1. Take stock. Know what personal information you have in your files and on your computers.
2. Scale down. Keep only what you need for your business.
3. Lock it. Protect the information that you keep.
4. Pitch it. Properly dispose of what you no longer need.
5. Plan ahead. Create a plan to respond to security incidents.

For further information, refer to:

<http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus69.pdf>

---

<sup>2</sup> <http://www.ftc.gov/reports/privacy3/fairinfo.shtm>

## Data Storage & Retention

---

Consumer data collected in an online lead generation form will vary based on the business need(s) of the advertiser. Consumer data may include but is not limited to:

- First name
- Last name
- Gender
- Date of birth
- Email address
- Physical address
- Phone number
- IP address
- Medical information
- Credit card data
- Social security number
- Other data such as education program of interest, mortgage value, household income, etc., that when combined with any of the above may become personally identifiable

❖ **All consumer data should be stored behind a firewall configuration one layer deeper than the primary firewall configuration.**

Firewalls are computer devices that control computer traffic allowed between a company's network (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within a company's internal trusted network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

Specifically, advertisers and publishers should have:

- A firewall configuration that restricts connections between untrusted networks and any system components in the consumer data environment. In ideal configurations, data is stored one network deeper than that which is connected to the internal firewall segment creating an additional layer of protection.
- Anti-virus software on systems, including personal computers and servers. It is understood that not all operating systems have viable anti-virus software available.
- The Payment Card Industry (PCI) Data Security Standard (DSS) Requirements and Security Assessment Procedures is a helpful reference for more information on firewall configuration:  
[https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml)

❖ **Advertisers and publishers should have a written data retention and disposal policy that conforms to their business and regulatory needs.**

Advertisers and publishers should have an up-to-date written data retention, disposal policy and procedure document. The document should include:

- List of possible consumer and campaign data stored
- Data classification for each data point
- Provisions for disposal of data when it is no longer needed for legal, regulatory, or business/operational reasons

The policy and procedures document should be reviewed on an annual basis at a minimum.

❖ **Advertisers and publishers should purge data as soon as possible within their business practices and regulatory guidelines.**

Consumer and campaign data should be retained only for the time period that is required for legal, regulatory, or business/operational purposes.

❖ **Advertisers and publishers should classify and encrypt their data.**

All data stored should be classified into groups. Each group may have different storage procedures and retention policies.

For example, Class 1 may include standard consumer PII data where the usage of Secure Sockets Layer (SSL) may not be required. Class 2 data may include medical data where SSL is required. Class 3 data may include financial data, such as credit card or social security number, where SSL is required. Each company should determine their definition of sensitive data and use MD5 Hash, 3DES or AES-encryption for secure storage.

❖ **User access to consumer data should be restricted and enforced with technical security measures.**

Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the consumers' PII. Managerial measures include internal organizational measures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes.

Formal policies and procedures should be in place to ensure that access to consumers' PII is restricted to individuals who have been properly authorized to access the data and that their specific job function requires access to the data. Access should be reviewed on a periodic basis to ensure that employees terminated and/or transferred have had their access privileges removed in a timely manner.

All users with access to consumer data should be assigned a unique ID to allow for audit trails. Logs should be maintained for every time someone has accessed highly sensitive consumer PII. Video cameras or other access control mechanisms to monitor

individual physical access to sensitive areas should be maintained and reviewed regularly.

Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers that are inaccessible by modem.

❖ **A formal compliance review of all network security procedures should be conducted annually at a minimum.**

A formal process for approving and testing network connections and changes to the firewall and router configurations in the path of accessing sensitive lead generation data should be conducted annually at a minimum. An up-to-date network diagram with all connections to consumer data, including any wireless networks, should be maintained and reviewed.

❖ **A formal compliance review of all data retention policies should be conducted annually at a minimum.**

A formal review process of all data retention policies, including data classifications and consumer and campaign data retention time periods, should be conducted annually at a minimum.

## Market Regulations

---

There are a myriad of regulations that should be considered as “best practices” when consumers’ personally identifiable information is protected. A short explanation of major industry regulations are provided below, but other market regulations for your specific industry should be considered:

❖ **If consumer credit card data is collected and stored, advertisers and publishers should be in compliance with the PCI Data Security Standard.**

The Payment Card Industry (PCI) Data Security Standard (DSS) Requirements and Security Assessment Procedures is a document that outlines requirements for companies that collect and store cardholder data. Requirements include: building and maintaining a secure network, protecting cardholder data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks, and maintaining an information security policy.

Refer to this document for full requirements:

[https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml)

❖ **If personal financial data is collected and stored, advertisers and publishers should be in compliance with the Gramm-Leach-Bliley Act.**

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act, is a law that governs the collection and disclosure of customers' personal financial information by financial institutions.

The GLB Act requires that:

1. A clear, conspicuous, and accurate statement of the company's privacy practices must be given to individual customers or consumers by mail or in-person delivery,
2. Consumers and customers have the right to opt out of having their information shared with certain third parties,
3. Limitations be placed on how anyone that receives nonpublic personal information from a financial institution can use or re-disclose the information,
4. Limitations be placed on how a company conducts business, and
5. Pretexting (the practice of obtaining customer information from financial institutions under false pretenses) is prohibited.

Refer to this document for full requirements:

<http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>

❖ **If consumer health data is collected and stored and the entity is a “covered entity”, advertisers and publishers should be in compliance with HIPAA.**

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) was effective on April 14, 2003. HIPAA applies to “covered entities,” which are health care providers, health plans (including employer’s sponsored plans), and healthcare clearing houses (e.g., billing agent). Essentially, a HIPAA covered entity cannot use or disclose protected health information for any purpose other than treatment, payment, or health care operations without either the authorization of the individual or under an exception in the HIPAA regulations. In particular, HIPAA requires covered entities to do the following:

1. Institute a required level of security for health information, including limiting disclosures of information to the minimum required for the activity;
2. Designate a privacy officer and contact person;
3. Establish privacy and disclosure policies to comply with HIPAA;
4. Train employees on privacy policies;
5. Establish sanctions for employees who violate privacy policies;
6. Establish administrative systems in relation to the health information that can respond to complaints, respond to requests for corrections of health information by a patient, accept requests not to disclose for certain purposes, track disclosures of health information;
7. Issue a privacy notice to patients concerning the use and disclosure of their protected health information;
8. Establish a process through an internal review board or a privacy board for a HIPAA review of research protocols; and
9. As a health care provider, include consent for disclosures for treatment, payment, and health care operations in treatment consent form (optional).

Refer to this document for full requirements:

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf>

❖ **If data from children under 13 is collected and stored, advertisers and publishers should be in compliance with COPPA.**

The Children's Online Privacy Protection Act of 1998 (COPPA) is a United States federal law effective on April 21, 2000 that applies to the online collection of personal information by persons or entities under U.S. jurisdiction from children under 13 years of age.

COPPA requires that commercial websites obtain verifiable parental consent before collecting personal information from a child under the age of 13 (age 12 and under). COPPA requires any online service operators to:

1. Post a privacy policy on the homepage of the Web site and link to the privacy policy on every page where personal information is collected,
2. Provide notice about the web site's information collection practices to parents and obtain verifiable parental consent before collecting personal information from children younger than 13,
3. Give parents a choice as to whether their child's personal information will be disclosed to third parties,
4. Provide parents access to their child's personal information and the opportunity to delete the child's personal information and opt-out of future collection or use of the information,
5. Not condition a child's participation in a game, contest or other activity on the child's disclosing more personal information than is reasonably necessary to participate in that activity, and
6. Maintain the confidentiality, security and integrity of personal information collected from children.

Refer to this document for full requirements:

<http://www.ftc.gov/ogc/coppa1.htm>

❖ **If student record data is collected and stored and the entity is an educational institution, advertisers and publishers should be in compliance with FERPA.**

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.
- Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.

- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):
  - School officials with legitimate educational interest;
  - Other schools to which a student is transferring;
  - Specified officials for audit or evaluation purposes;
  - Appropriate parties in connection with financial aid to a student;
  - Organizations conducting certain studies for or on behalf of the school;
  - Accrediting organizations;
  - To comply with a judicial order or lawfully issued subpoena;
  - Appropriate officials in cases of health and safety emergencies; and
  - State and local authorities, within a juvenile justice system, pursuant to specific State law.

Refer to this document for full requirements:

<http://www.ed.gov/policy/gen/guid/fpc/ferpa/index.html>

❖ **Any advertiser or publisher that is part of a publicly held company and meets certain requirements must be in compliance with Sarbanes-Oxley.**

Sarbanes-Oxley Act Section 404 is listed under Title IV of the act (Enhanced Financial Disclosures), and pertains to 'Management Assessment of Internal Controls'.

“Issuers are required to publish information in their annual reports concerning the scope and adequacy of the internal control structure and procedures for financial reporting. This statement shall also assess the effectiveness of such internal controls and procedures. The registered accounting firm shall, in the same report, attest to and report on the assessment on the effectiveness of the internal control structure and procedures for financial reporting.”

One of the key controls addressed through SOX is Data Security / Access Control.

Refer to this document for full requirements:

[http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107\\_cong\\_bills&docid=f:h3763enr.txt.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.txt.pdf)

## Network Controls

---

Network Controls ensure the security of proprietary networks through the monitoring of access to available network and compliance with a defined security policy.

❖ **Responsibility for data security should be incorporated into an internal job function.**

It is essential that oversight of data security procedures is incorporated into an internal job function within the company, even if a third party is utilized for execution.

❖ **A network security policy listing all actionable procedures, recurring or potential, should be in formally written documents and reviewed annually.**

While network security policy should be owned by managers of IT/Technology within the company, the review process is best served in a cross-functional format. Other departments that take part in the responsibility of network security and/or would be directly impacted by any changes to network security policy should be involved. An annual review of your network security policy should be conducted to assess current protocols and address any upcoming changes.

❖ **Details of all connections should be outlined in a current network diagram.**

Confusion over the structure of the network can be avoided with a network diagram demonstrating all connections to consumer data, including wireless networks in addition to a detailed list of all of the data elements that are also considered to be critical to the business.

❖ **Network control procedures should describe the formal process to approve and test external network connections and changes to their configuration.**

Examples of procedures to be outlined via written documentation:

- Always document changes to the firewall and router configurations
- A written time period for review of all firewall configurations will help to ensure timely assessments
- Maintain a written response plan for security incidents
- Create accountability for non-standard network events through the use of logs

❖ **Security testing should outline a list of tasks between the websites and general networks, with testing procedures in place.**

Security testing should include:

- Scans of internal and external networks along with a check of the logs will serve to detect open ports and close off unnecessary access
- Annual attack and penetration testing should be performed on the network level (for those networks in the path to access sensitive lead generation data) to test existing security protocols and identify any potential gaps in coverage
- Testing & auditing of security protocols can assist with improving and monitoring of the above