



# IAB Lead Generation Data Transfer Best Practices

Released August 15, 2007

Developed and endorsed by the following members of the IAB Lead Generation Committee:

360i  
Active Response Group  
Cox Newspapers, Inc.  
Edmunds.com  
Geary Interactive  
IDG  
Innovation Ads  
Jordan Edmiston Group, Inc.  
Motive Interactive Inc.  
Move, Inc. Related Services  
NextAction

Permission Data  
PointRoll  
Q Interactive  
Reed Business  
Return Path  
SendTec  
TARGUSinfo  
The AMC Group  
ValueClick Media  
Vizi Media  
WebTrends



# IAB Lead Generation Data Transfer Best Practices

## Executive Summary

---

The IAB Lead Generation Committee (the “Committee”) has developed this document to educate advertisers/marketers who purchase lead generation services (“Advertisers”) and companies providing lead generation services to those Advertisers (“Providers”) on security and operational best practices regarding transfer of lead information.

**These Best Practices have two main considerations:**

- 1. SECURITY – All lead generation data should be transferred and received in an encrypted format**
- 2. COMMON FORMAT AND SETUP – All lead generation data should be transferred in a common format via common, secure internet technologies**

### OVERVIEW

This document will outline (1) the benefits of the Committee’s recommendations, (2) current and emerging state and federal laws, rules, and regulations for lead generation and data transmittal practices, (3) proposed standards for the handling of consumers’ Personally Identifiable Information, and (4) a step-by-step method for receipt of data, along with the common field names to be used.

The absence of lead generation guidelines makes compliance with applicable laws, rules, and regulations more difficult. Therefore, these Data Transfer Best Practices have been written to improve the security of consumers’ Personally Identifiable Information, standardize lead transmittal practices, and improve operational efficiencies for the benefit of Advertisers, Providers, and ultimately, consumers.

In addition, many Advertisers are currently not equipped to receive data in an encrypted format. The Committee encourages Advertisers to adapt their systems to enable receipt of leads from Providers in accordance with the best practices set forth below. The Committee also encourages Providers to be equipped to transfer data in an encrypted format to those Advertisers already capable of receiving data in such a manner.

### OBJECTIVES

The IAB Lead Generation Committee’s goals in creating this document are:

- 1) To standardize the transfer and receipt of data between Advertisers and Providers in an encrypted format, where the safety and integrity of consumers’ Personally Identifiable Information is assured;
- 2) To assist Advertisers and Providers in complying with all existing and emergent laws, rules, and regulations at both the state and federal levels; and
- 3) To improve operational efficiency by encouraging the standardization of the formats and materials used by Advertisers to receive Data from Providers

## IAB Lead Generation Data Transfer Best Practices

**IMPORTANT NOTE:** This document focuses on the transfer of data between a Provider and an Advertiser. It does not cover the full lifecycle of lead generation and usage, which would also include stages such as data collection and storage by both Provider and Advertiser.

### Encryption and Security Best Practices

---

**All Advertisers should receive data in an encrypted format in order to comply with all laws and ensure the security and privacy of the data. In addition, Providers should be able to offer full support to Advertisers by always delivering data encrypted to those Advertisers with the capacity to accept data in an encrypted format.**

Providers' ability to transport the data in an encrypted format can be limited by whether Advertisers have the technological capacity to accept it. The Committee recommends that, wherever possible, Providers try to encourage their clients to adopt technology that is capable of accepting data in an encrypted format.

#### **DATA ENCRYPTION RECOMMENDATION: REAL-TIME DATA**

**The Committee recommends that best efforts be made to transfer data in real-time, and that all real-time transfer of data be done with encryption equal to or greater than 128-bit SSL encryption (through HTTPS web services, etc).**

#### **DATA ENCRYPTION RECOMMENDATION: BATCH DATA**

**The Committee recommends that, if real-time data transfer is not possible, all batch data be transferred via Secure FTP** because it is the most practical of commercially available, cost effective, encrypted data transfer methods. Standard FTP does not use strong enough authentication to ensure proper security and is susceptible to "middle-man" interception of data. Secure FTP software improves the security of standard FTP technologies by using encryption such as SSL and X.509 certificates.

There are various providers of Secure FTP software but it is important to understand that not all solutions use the same encryption techniques and standards. There is some debate within IT professionals which software providers are better than others and it is up to each Advertiser or Provider to evaluate the merits of individual vendors. However, many software vendors are federally certified under the FIPS-140 requirements which may be considered strong security requirements. Vendors that have received FIPS-140 certifications can be found here:

<http://csrc.nist.gov/cryptval/140-1/1401vend.htm>

If Secure FTP is not possible, the only other method of batch data delivery recommended by the group is PGP or other public key-based cryptology protocols with a minimum of 128-bit encryption. Every file transferred would need to be encrypted via a PGP-like technology before it could be transferred using non-secure methods. This would require both parties to exchange public keys and can be more complicated than implementing a Secure FTP framework.

#### **SAFE HARBOR LAWS AND ENCRYPTION**

At the time of this writing, at least 38 states and the District of Columbia have laws that require consumer notification in the event of a data breach. Each state law has its own varying scope and complexities, creating an onerous burden for any online marketer, as well as potential confusion for consumers.

In addition, there is likely to be national legislation that could add to the compliance burden. However, all of the state laws and the proposed national legislation have one thing in common: a data encryption safe harbor. Although advertisers are expected to provide encryption that cannot be reasonably or easily compromised, implementing properly secure encryption eliminates the need for advertisers to manage multiple compliance requirements, streamlines operations, reduces the chances of data breach, and can provide additional protection in accordance with existing safe harbor laws.

It is important to note that the entire lifecycle of lead generation, including data collection, storage, and transfer for all parties involved must be considered when investigating Safe Harbor requirements.

# IAB Lead Generation Data Transfer Best Practices

FOR MORE INFORMATION, PLEASE VISIT SOME OF THE FOLLOWING RESOURCES:

National Institute of Standards and Technology: Computer Security Resource Center  
[www.csrc.nist.gov](http://www.csrc.nist.gov)

NIST's Risk Management Guide for Information Technology Systems  
[www.csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf](http://www.csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf)

Department of Homeland Security's National Strategy to Secure Cyberspace  
[www.dhs.gov/xlibrary/assets/National\\_Cyberspace\\_Strategy.pdf](http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf)

SANS (SysAdmin, Audit, Network, Security) Institute's Twenty Most Critical Internet Security Vulnerabilities  
[www.sans.org/top20](http://www.sans.org/top20)

Center for Internet Security (CIS)  
[www.cisecurity.org](http://www.cisecurity.org)

Protecting Personal Information: A Guide For Business  
<http://www.ftc.gov/bcp/edu/pubs/business/privacy/bus69.pdf>

## Data Transfer Best Practices

---

Depending on the needs and technology of the client, the Committee has developed recommendations for improving the execution of both batch delivery and real-time delivery of leads.

### DATA TRANSFER RECOMMENDATION: *REAL-TIME DELIVERY*

There are many methods that are currently being used by advertisers and companies for transferring leads in real-time. Currently the most ubiquitous method to transfer one or more records securely in real-time involves the use of HTTP and SSL. Because of this, **the Committee recommends that data be transferred via an HTTPS POST using Secure-Socket Layers (SSL) for security.**

The Committee also recommends the following:

#### 1. Naming Conventions

The naming conventions found in the "Common Data Field Naming Best Practices" section should be followed as needed when selecting field names for the data to be transferred.

### **PERSONALLY IDENTIFIABLE INFORMATION (PII)**

Instilling confidence in consumers about their ability to transact with an advertiser's brand is a foundational element that supports the growth of interactive advertising, marketing and commerce. This confidence can be built along a number of dimensions, but none as critical as privacy and security.

Advertisers should be sensitive to the issue of consumer privacy and should limit their collection, combination, transfer or use of marketing data for the specific purpose(s) needed. Marketing data should be used only for marketing purposes. Again, the Committee recommends employing encryption-enabled protocols, like Secure Sockets Layer (SSL) or other similar encoding technologies, as a best practice when collecting and transferring customer data.

It is important to understand that all Personally Identifiable Information (PII) should be treated with the utmost seriousness and security (as per section "Encryption and Security Best Practices").

Additional considerations when dealing with PII include:

Advertisers should be guided by the reasonable expectations of confidentiality/privacy when transferring any combination of data that could identify a unique individual. **Specifically, all advertisers should abide by the promises made to**

## 2. Data Formatting

### a) Name-Value Pairs

At the current time, name-value pairs are considered quick, efficient, and simple for all parties to implement and they are therefore the preferred recommendation for posting information. Name-value combinations using the naming conventions found in the “Data Field Naming Best Practices” section will create large operational efficiency gains for the largest number of partners.

### b) XML

As the industry matures and more lead generation providers and clients are looking to improve operational efficiencies, a universal standard for passing data back and forth will simplify setup of vendors and allow both providers and clients to change their internal systems, databases, and technologies without disrupting the way data is transferred between parties. The eXtensible Markup Language (XML) was designed for this purpose and is a flexible, self-defining language for describing data. As such, the Committee recommends that data begin to be formatted using XML and begin exploring with their partners the use of an XML schema that follows the naming conventions found in the “Data Field Naming Best Practices” section.

## 3. Data Transfer

The data transfer should be accomplished in one step (within one “handshake”) and:

- 1) There should be no redirects to other pages
- 2) If it is necessary for multiple locations (post-to webpages, etc) and handoffs to be involved in the data transfer process (commonly referred to as “ping posts”) this should be handled by the receiving server.

## 4. Response Communications

The receiving server should always provide a recognizable response via HTTP that, at a minimum, indicates that the data was received. No visual formatting should be used (tables, CSS, etc.) The response format should be in either plain HTML or XML:

- a) If multiple records were transferred at once, an XML response is preferred with acceptance/rejection indicated for each record, using the primary key field as a unique record identifier.
- b) If XML is not used, then a response in HTML should be returned with a code that indicates if the record was received. Furthermore, if possible, the response should indicate whether the record was

### consumers in their privacy

**policies.** It is important to note that the Federal Trade Commission and state attorneys general have noted, time and again, that they view **an organization’s privacy policy like a contract between that organization and consumers.** Any violations of that contract are subject to actions from either or both the FTC and the various state attorneys general.

***Please note:** Advertisers who plan to adopt these Encryption and Security Best Practices should ensure that their operational activities support each statement made in their privacy policies before making any change to the content of those privacy policies. In other words, Advertisers’ actual business practices must match the content of their privacy policies in order to comply with applicable laws, rules, and regulations concerning on-line disclosures.*

Advertisers should take reasonable precautions to transfer this data in a manner that is consistent with the reasonable security expectations of consumers. Advertisers should rely on and abide by the notice they provide in their policies regarding transfer of PII to third parties (e.g., name, address, contact info, marketing preferences, and/or other data). Consumers should be provided with choice about the permitted transfer of any PII. Consumer choice should be honored in any data transfer. The Committee recommends that advertisers maintain in-house suppress lists as a mechanism to honor such consumer choice.

## IAB Lead Generation Data Transfer Best Practices

accepted or rejected, with the rejection reason included. The unique identifier for the given records should also be returned. Samples are below:

```
<HTML>Primary_key=123456
DataResponse=Accepted</HTML>
<HTML>Primary_key=123456
DataResponse=Rejected</HTML>
<HTML>Primary_key=123456
DataResponse=Rejected -
Duplicate</HTML>
<HTML>Primary_key=123456
DataResponse=Rejected – Bad
Address</HTML>
<HTML>Primary_key=123456
DataResponse=Rejected – Bad
Phone</HTML>
<HTML>Primary_key=123456
DataResponse=Rejected – Not
qualified</HTML>
<HTML>Primary_key=jsmith@smith.com
DataResponse=Rejected – CC bad</HTML>
...
```

### 5. Error handling

If the receiving server does not respond or is returning a data response that is not recognized, the sending server will retry sending the data every hour up to 12 hours.

Credit card, Social Security, unique government identification numbers of any kind, health and medical information, information about children, other financial account information and debit account numbers are examples of sensitive personally identifiable information, especially if combined with name and address fields. Any use of these identifiers should be strictly limited to uses that are within consumers' reasonable expectations of security. Ask yourself: Can I authenticate my customer with just the last four digits of a Social Security Number? Do I have to abide by Payment Card Industry Data Security Standards (PCI-DSS)? What level of PCI-DSS governs my organization? What is the least amount of data I need to achieve the level of relevance that my consumers expect? Adhering to industry best practices, limiting use and transfer of these sensitive data elements will limit your organization's exposure to identity theft, costly charge-backs, and potential civil liability.

### DATA TRANSFER RECOMMENDATION: *BATCH DELIVERY*

The Committee recommends that batch file delivery of lead data be used only when the party or parties involved are unable to accept data using any of the other real-time methods outlined in this document.

If batch delivery is used the following formatting is recommended.

- All batch files should be delivered using CSV (Common-separated Values) format
  - Quotes should be placed around all data to avoid values with commas being misread
- All files should use standard UNIX line return (\n)
- Each file should include a header row that with field names that follow the naming conventions set forth in this document's "Data Field Naming Best Practices" section.
- The first column of all files should start with a unique record identifier / primary key
- The file name should include the source company name, campaign name and the date the file was created using the format

## IAB Lead Generation Data Transfer Best Practices

<source>\_<campaign>\_<year>\_<month>\_<day>\_<hour>\_<minutes>\_<seconds> (for example "carloan\_2007\_01\_18.csv")

**FOR MORE INFORMATION ON XML, PLEASE VISIT SOME OF THE FOLLOWING RESOURCES:**

An introduction to XML Basics

<http://www.peachpit.com/articles/article.asp?p=31286&seqNum=8&rl=1>

The XML FAQ

<http://www.ucc.ie/xml/>

W3C XML Resource

<http://www.w3.org/XML/>

## Common Data Field Naming Best Practices

---

As part of the industry's effort to improve operational efficiency, the Committee has developed a recommendation for data field naming conventions. *(Note: If an industry segment has already developed specialized standard naming conventions such as the automotive "Auto-lead Data Format [ADF]", these field names should be considered alternatives, not replacements)* The Committee recommends that the following list of common data fields be named in the following way when used, regardless of transfer method (XML or HTML Name-Value Pairs):

**Note:** All naming of data fields should be normalized to lowercase and underscore-delimited.

### 1. Date / Timestamp

The date and time the lead was received.

<timestamp>

The date and timestamp should conform to the following canonical data format:

<year>\_<month>\_<day>\_<hour>\_<minutes>\_<seconds>

Example: 2007\_12\_04\_18\_12\_58 (NOTE: 24-hour time)

*NOTE: Date and timestamp information may also be transferred as separate name-value pairs if deemed necessary or expedient.*

### 2. Timezone

The timezone that the time was taken in. Default/no-value equates to Greenwich Mean Time. All other timezone values would be relative to Greenwich.

<timezone>

Example: -05:00 (for Eastern standard time)

### 3. First Name

First name identifies the person by their name:

## IAB Lead Generation Data Transfer Best Practices

*<first\_name>*

Example:

- Jane
- John

#### 4. Last Name

Last name identifies the person by their surname:

*<last\_name>*

Example:

- Doe
- John

#### 5. Address 1

The primary address identifies the location to which physical mail (snail) may be delivered.

*< address1>*

Example:

- 555 Main Street>

#### 6. Address 2

The secondary address identifies a subordinate location to Address 1 which physical mail (snail) may be delivered.

*<address2 >*

Example:

- Apartment 3
- building 4
- park square building

#### 7. City

The city identifies the named-geographic location in which the lead lives or works.

*<city>*

Example:

- Athens
- Vienna
- dubai
- port ligat
- New York

#### 8. State

## IAB Lead Generation Data Transfer Best Practices

The state identifies the state or other similar international concept (jurisdiction, quadrant, province, and so on) in which the lead lives or works.

*<state>*

**Example:**

- RI
- AZ
- New Brunswick

### 9. Zip / Postal Code

Zip / Postal Code identifies the five-digit, three-digit, nine-digit, or other alpha-numerical zip-code based identifier associated with Address1, Address2, and State. This should not include additional US Zip+4 digits.

*<postal\_code>*

**Example:**

- 902
- 90210
- SW18 4HB

### 10. Zip+4

For United States addresses, an additional field of four extra zip digits can also be fairly common.

*<zip\_4>*

Example: 2065

### 11. Country

Country identifies the geography for the lead's Address1, Address1, State, and Zip Code.

*<country>*

**Example:**

- canada
- CA
- United States
- US

### 12. Contact Information

- Home Phone
- Land phone
- Work Phone
- Cell Phone
- Alt Phone
- Email

## IAB Lead Generation Data Transfer Best Practices

The phone number is the series of digits that enable land-based, cellular, or VOIP telephony connections:

- `<phone_home>` : 1112223333, Intl: 44213092302
- `<phone_work>` : 7778889999
- `<phone_cell>` - 1234567890
- `<phone_alt>` - 9876543210
- `<email>` - [john\\_doe@something.com](mailto:john_doe@something.com), [doe@nothing.com](mailto:doe@nothing.com)
- `<email_confirm>` - [john\\_doe@something.com](mailto:john_doe@something.com), [doe@nothing.com](mailto:doe@nothing.com)

### 13. Company Name

The company for which a contact works.

`<company_name>`

Example:

- IAB
- Acme Consulting

### 14. Best Time To Call

Identifies the most convenient time for the lead to be contacted and the most appropriate time for the advertiser to contact the lead based on GMT and military time.

`<best_call_time>`

Example:

- 03:00
- 22:14

### 15. Highest Level of Education

Identifies the highest educational level that the lead has earned.

`<highest_education_level>`

Example of possible values:

- Some primary education
- Primary education graduate
- ged
- some college
- college graduate
- masters degree
- phd
- professional degree

### 16. Preferred Contact Method

Indicates the best method for communicating with the lead

`<preferred_method>`

Example: home phone, email

## IAB Lead Generation Data Transfer Best Practices

### 17. High School Grad Year

Indicates the calendar year in which the lead graduated from high school

*<high\_school\_graduate\_date>*

Example:

- 1967
- 1992
- 2007

### 18. Collateral Requested

Identifies the informational object requested for download by the lead.

*<collateral\_requested>*

Example of possible types:

- document
- White paper
- podcast
- marketing literature
- sales literature
- Model

### 19. SS# or Government Issued Identifier

Identifies the social security number or government ID for the lead

*<ssn>*

Example:

- 123456789

### 20. Mother's Maiden Name

Identifies the surnames of the lead's mother before and if she is/was married.

*<mother\_maiden\_name>*

Example:

- Smith
- Jones
- smith jones

### 21. Date of Birth

Indicates the day, month, and year that the lead was born.

*<dob>*

Example: 2007\_12\_20

### 22. IP Address

Indicates the standard internet protocol address.

*<ip\_address>*

Example:

- 12.23.123.123

### 23. Product Selection

Indicates the product that was selected by the lead during the capture process. The product identified must use no more than 64 alphanumeric, lowercase, underscore delimited characters.

*<product\_selection>*

Example:

- My white paper
- Podcast 32456\_n
- p\_4\_90\_290\_poe\_x3i

### 24. Product Category

Indicates the category assigned to the product that was selected by the lead during the capture process. The product identified must use no more than 64 alphanumeric, lowercase, underscore delimited characters.

*<product\_category>*

Example:

- My prod cat
- White papers
- podcast\_n\_67\_n
- c\_6g\_9t0\_2290\_poe\_x3i

### 25. Number of Children

Indicates the number of children dependent on the lead.

*<number\_children>*

Example:

- 1
- 2
- 3

### 26. Credit Card Number

Indicates the credit card number submitted via 128-bit encryption by the lead during the capture process. The credit card number is a 15 or 16 character, integer string.

*<cc\_number>*

Example:

- 1111222233334444
- 44446666665555

### 27. Credit Card Expiration

Month and year of expiration

*<cc\_exp>*

Example: 2007\_01

### 28. Credit Card Security Code

3 or 4 digit security code on back (or front with Amex) of card

*<cc\_securitycode>*

Example:

- 2532
- 801

### 29. Primary key – User ID, RecordID

Identifies a unique series of alphanumeric characters that defines a primary identifier, which can be decoded via a lookup. The primary key may reference any system object in your lead capture process, such as a userid, recordid, customerid, or lookup table.

*<primary\_key>*

Example:

- 1a
- 1\_2
- 123
- 1a234
- 123A5
- a23456
- 123a\_567
- 12345678
- 1\_2\_a
- 1\_a\_2\_3\_a and so on

### 30. Campaign / Keycode

A communication, such as direct mail or a print ad, may mention this code, which is a unique key identifying some resource or object.

Identifies a unique series alphanumeric characters that defines a unique primary identifier. The campaign or keycode may reference a lookup table.

*<campaign\_keycode>*

Example:

- 1a
- 1\_2
- 123
- 1a234
- 123a\_567
- 12345678
- 1\_2\_a
- 1\_a\_2\_3\_a and so on

### 31. Company Code – Originator code

Identifies a unique series of alpha-numeric characters that defines the company. The campaign or keycode may reference a lookup table.

*<company\_code>*

## IAB Lead Generation Data Transfer Best Practices

Example:

- 1a
- 1\_2
- 123
- 1a234
- 123A5
- a23456
- 123a\_567
- 12345678
- 1\_2\_a
- 1\_a\_2\_3\_a

### 32. Website/URL

The website, if different from the Company Code, where the lead originated

<url>

Example:

- [www.google.com](http://www.google.com)
- [www.innovationads.com](http://www.innovationads.com)
- [www.careersandeducation.com](http://www.careersandeducation.com)

## Contacts

---

### **Jeremy Fain**

Director of Industry Services

IAB

212-380-4724

[jeremy@iab.net](mailto:jeremy@iab.net)

### **Luke Lockett**

Associate Manager of Industry Services

IAB

212-380-4715

[luke@iab.net](mailto:luke@iab.net)

### **Gayle Guzzardo**

Senior Vice President of Product Management

Q Interactive

IAB Lead Generation Committee Chair

[gguzzardo@qinteractive.com](mailto:gguzzardo@qinteractive.com)