

## Membership Application Checklist For Business Owner Profile (BOP) Only

(must be completed prior to account activation)

Date: \_\_\_\_\_

Company Name: \_\_\_\_\_

Type of ownership (indicate one): ☐ Partnership ☐ Sole Owner ☐ Nonprofit ☐ Corporation ☐ LLC

Physical Address (no P.O. box numbers please): \_\_\_\_\_

City/State/Zip: \_\_\_\_\_ How long? \_\_\_\_ years \_\_\_\_ months

What type of business location are you in? ☐ Commercial ☐ Residential

Company Phone: \_\_\_\_\_ Contact Phone: \_\_\_\_\_ Fax: \_\_\_\_\_

Email: \_\_\_\_\_ Federal Tax ID: \_\_\_\_\_

Previous Address (*If less than 5 years at current*): \_\_\_\_\_

City/State/Zip: \_\_\_\_\_ How long? \_\_\_\_ years \_\_\_\_ months

Do you own or lease the building in which you are located (please check one): ☐ Own ☐ Lease

### If sole owner or partnership, please complete this section:

I understand that the information provided below will be used to obtain a consumer credit report and my creditworthiness may be considered when making a decision to grant membership

Principal Name: \_\_\_\_\_ Title/Position: \_\_\_\_\_

Phone number: \_\_\_\_\_

Affiliated or Parent Company Name: \_\_\_\_\_

Contact Name: \_\_\_\_\_ Title: \_\_\_\_\_

Street Address: \_\_\_\_\_ Phone: \_\_\_\_\_

City/State/Zip: \_\_\_\_\_

What is the nature of your business? \_\_\_\_\_

How long has your company been in business? \_\_\_\_ years \_\_\_\_ months

What will you be using the Business Owner Profile (BOP) reports for? \_\_\_\_\_

\_\_\_\_\_

Please describe the **specific** purpose for which Experian product information will be used. (What will you do with the information obtained?)

**This section MUST be completed.**

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_



Do you have a web site? ☐ Yes ☐ No If Yes, provide Web address \_\_\_\_\_

If you will be pulling credit reports, # of estimated credit reports you will access monthly: \_\_\_\_\_

How will you access credit reports? ☐ Personal Computer ☐ Phone/Fax Other \_\_\_\_\_

I have received and understand my responsibilities under the Fair Credit Reporting Act. ☐ Yes ☐ No

I have received and understand my security responsibilities as outlined in the Access Security Requirements as provided by DFI with regard to credit reports received. ☐ Yes ☐ No

**MEMBER USE LIMITATION** - Client hereby certifies and agrees that its request for consumer credit information arises out of a legitimate business credit transaction involving the entity as to whom a credit profile is sought, and, Client further certifies and agrees that consumer credit data which is sought and received shall be held in strictest of confidence and will not be resold or otherwise distributed to any other third parties, except as otherwise required by law. In the event there is a change in federal and/or state laws governing this area of reporting, Client agrees to sign an amended agreement if it desires to continue receiving consumer reports.

Are you, or your business, associated or affiliate with any of the following?

Credit repair	<input type="checkbox"/> Yes <input type="checkbox"/> No	Private Investigation	<input type="checkbox"/> Yes <input type="checkbox"/> No
Media	<input type="checkbox"/> Yes <input type="checkbox"/> No	Legal Services	<input type="checkbox"/> Yes <input type="checkbox"/> No
Law Enforcement	<input type="checkbox"/> Yes <input type="checkbox"/> No	Asset Location	<input type="checkbox"/> Yes <input type="checkbox"/> No
Bail Bonds	<input type="checkbox"/> Yes <input type="checkbox"/> No	Dating Service	<input type="checkbox"/> Yes <input type="checkbox"/> No

**REFUSAL OF SERVICE** - Data Facts reserves the right to refuse "Consumer Credit Reports" services to any client of Data Facts who violates the companies established rules of procedure or any provision of Public Law 91-508, known as the Fair Credit Reporting Act and other applicable laws. Client hereby further agrees to comply with all federal, state and local statues, regulations and rules applicable to it, including, without limitation the FCRA, with any changes enacted to FCRA during the term of this Agreement, the Gramm Leach Bliley Act and its implementing regulations, any state or local laws governing the disclosure of consumer credit information

**Please provide a business banking references, as well as two business credit references, excluding credit card accounts:**

**Business Checking Account Reference:** \_\_\_\_\_ Date Opened: \_\_\_\_\_  
 Acct #: \_\_\_\_\_ Contact Name: \_\_\_\_\_  
 Address: \_\_\_\_\_ Phone: \_\_\_\_\_  
 Comments: \_\_\_\_\_

**Business Reference:** \_\_\_\_\_ Date Opened: \_\_\_\_\_  
 Acct #: \_\_\_\_\_ Contact Name: \_\_\_\_\_  
 Address: \_\_\_\_\_ Phone: \_\_\_\_\_  
 Comments: \_\_\_\_\_

**Business Reference - :** \_\_\_\_\_ Date Opened: \_\_\_\_\_  
 Acct #: \_\_\_\_\_ Contact Name: \_\_\_\_\_  
 Address: \_\_\_\_\_ Phone: \_\_\_\_\_  
 Comments: \_\_\_\_\_

**Company Name:** \_\_\_\_\_

**Name of Authorized Signor:** \_\_\_\_\_ **Title:** \_\_\_\_\_

**Authorized Signature:** \_\_\_\_\_ **Date:** \_\_\_\_\_

**All documents must be physically signed.**



## EXHIBIT A

### FCRA REQUIREMENTS

Federal Fair Credit Reporting Act (as amended by the Consumer Credit Reporting Act of 1996)

Although the FCRA primarily regulates the operations of consumer reporting agencies, it also affects you as a user of information.

You can review a copy of the FCRA at <http://www.ftc.gov/os/statutes/fcrajump.htm>. We suggest that you and your employees become familiar with the following sections in particular:

- 604 Permissible Purposes of Reports
- 607 Compliance Procedures
- 610 Conditions and Form of Disclosure to Consumers
- 611 Procedure in Case of Disputed Accuracy
- 615 Requirement on users of consumer reports
- 616 Civil liability for willful noncompliance
- 617 Civil liability for negligent noncompliance
- 619 Obtaining information under false pretenses
- 620 Unauthorized Disclosure by Officers or Employees
- 621 Administrative Enforcement
- 623 Responsibilities of Furnishers of Information to Consumer Reporting Agencies
- 628 Disposal of Records

Each of these sections is of direct consequence to users who obtain reports on consumers.

As directed by the law, credit reports may be issued only if they are to be used for extending credit, review or collection of an account, employment purposes, underwriting insurance or in connection with some other legitimate business transaction such as in investment, partnership, etc. It is imperative that you identify each request for a report to be used for employment purposes when such report is ordered. Additional state laws may also impact your usage of reports for employment purposes.

Data Facts, Inc. strongly endorses the letter and spirit of the Federal Fair Credit Reporting Act. We believe that this law and similar state laws recognize and preserve the delicate balance between the rights of the consumer and the legitimate needs of commerce.

In addition to the Federal Fair Credit Reporting Act, other federal and state laws addressing such topics as computer crime and unauthorized access to protected databases have also been enacted. As a prospective user of consumer reports, we expect that you and your staff will comply with all relevant federal statutes and the statutes and regulation of the states in which you operate.

INITIALS: \_\_\_\_\_



## ACCESS SECURITY REQUIREMENTS

We must work together to protect the privacy and information of consumers. The following information and security measures are designed to reduce unauthorized access to consumer information. It is your responsibility to implement these controls. If you do not understand these requirements or need assistance, it is your responsibility to employ an outside service provider to assist you. Capitalized terms used herein have the meaning given in the Glossary attached hereto. Data Facts, Inc. reserves the right to make changes to the Access Security Requirements without notification. The information provided herewith provides minimum baselines for information security.

In accessing Data Facts, Inc. services, you agree to follow these security requirements:

### 1. Implement Strong Access Control Measures

- 1.1 Do not provide your Data Facts, Inc. Subscriber Codes or passwords to anyone. No one from Data Facts, Inc. will ever contact you and request your Subscriber Code number or password.
- 1.2 Proprietary or third party system access software must have Data Facts, Inc. Subscriber Codes and password(s) hidden or embedded. Account number(s) and password(s) should be known only by supervisory personnel.
- 1.3 You must request your Subscriber Code password be changed immediately when:
  - \* any system access software is replaced by system access software or is no longer used;
  - \* the hardware on which the software resides is upgraded, changed or disposed of
- 1.4 Protect Data Facts, Inc. Subscriber Code(s) and password(s) so that only key personnel know this sensitive information. Unauthorized personnel should not have knowledge of your Subscriber Codes(s) and password(s).
- 1.5 Create a separate, unique user ID for each user to enable individual authentication and accountability for access to the Data Facts, Inc. infrastructure. Each user of the system access software must also have a unique logon password.
- 1.6 Ensure that user IDs are not shared and no Peer-to-Peer sharing is enabled on those users' profiles.
- 1.7 Keep user passwords Confidential.
- 1.8 Develop strong passwords that are:
  - \* Not easily guessable (i.e. your name or company name, repeating numbers and letters or consecutive numbers and letters)
  - \* Contain a minimum of seven (7) alpha/numeric characters for standard user accounts
- 1.9 Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations.
- 1.10 Active logins to the Data Facts, Inc. system must be configured with a 30 minute inactive session timeout.
- 1.11 Restrict the number of key personnel who have access to credit information.
- 1.12 Ensure that personnel who are authorized access to credit information have a business need to access such information and understand these requirements to access such information are only for the permissible purposes listed in the Permissible Purpose Information section of your membership application.
- 1.13 Ensure that you and your employees do not access your own credit reports or those reports of any family member(s) or friend(s) unless it is in connection with a credit transaction or for another permissible purpose.
- 1.14 Implement a process to terminate access rights immediately for users who access Data Facts, Inc. credit information when those users are terminated or when they have a change in their job tasks and no longer require access to credit information.
- 1.15 After normal business hours, turn off and lock all devices or systems used to obtain credit information.
- 1.16 Implement physical security controls to prevent unauthorized entry to your facility and access to systems used to obtain credit information.

### 2. Maintain a Vulnerability Management Program

- 2.1 Keep operating system(s), Firewalls, Routers, servers, personal computers (laptop and desktop), and all other systems current with appropriate system patches and updates.
- 2.2 Configure infrastructure such as Firewalls, Routers, personal computers and similar components to industry best security practices, including disabling unnecessary services or features, removing or changing default passwords, IDs, and sample files/programs, and enabling the most secure configuration features to avoid unnecessary risks.
- 2.3 Implement and follow current best security practices for Computer Virus detection scanning services and procedures:
  - \* Use, implement and maintain a current, commercially available Computer Virus detection/scanning product on all computers, systems and networks.
  - \* If you suspect an actual or potential virus, immediately cease accessing the Data Facts, Inc. system and do not resume the inquiry process until the virus has been eliminated.
  - \* On a weekly basis, at a minimum, keep anti-virus software up-to-date by vigilantly checking or configuring auto updates and installing new virus definition files.
- 2.4 Implement and follow current best security practices for computer anti-Spyware scanning services and procedures:
  - \* Use, implement and maintain a current, commercially available computer anti-Spyware scanning product on all computers, systems and networks.
  - \* If you suspect actual or potential Spyware, immediately cease accessing the Data Facts, Inc. system and do not resume the inquiry process until the virus has been eliminated.
  - \* Run a secondary anti-Spyware scan upon completion of the first scan to ensure all Spyware has been removed from your computers.
  - \* Keep anti-virus software up-to-date by vigilantly checking or configuring auto updates and installing anti-Spyware definition files weekly, at a minimum. If your company's computers have unfiltered or unblocked access to the Internet (which



prevents access to some known problematic sites), then it is recommended that anti-Spyware scans be completed more frequently than weekly.

### **3. Protect Data**

- 3.1 Develop and follow procedures to ensure that data is protected throughout its entire Information Lifecycle (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e. tape, disk, paper, etc.)
- 3.2 All Data Facts, Inc. data is classified as Confidential and must be secured to this requirement at a minimum.
- 3.3 Procedures for transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.
- 3.4 Encrypt all Data Facts, Inc. data and information when stored on any laptop computer and in the database using AES or 3DES with 128-bit key Encryption at a minimum.
- 3.5 Only open email attachments and links from trusted sources and after verifying legitimacy.

### **4. Maintain an Information Security Policy**

- 4.1 Develop and follow a security plan to protect the Confidentiality and integrity of personal consumer information as required under the GLB Safeguard Rule.
- 4.2 Establish processes and procedures for responding to security violations, unusual or suspicious events and similar incidences to limit damage or unauthorized access to information assets and to permit identification and prosecution of violators.
- 4.3 The FACTA Disposal Rules requires that you implement appropriate measures to dispose of any sensitive information related to consumer credit reports and records that will protect against unauthorized access or use of that information.
- 4.4 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security within your organization.

### **5. Build and Maintain a Secure Network**

- 5.1 Protect Internet connections with dedicated, industry-recognized Firewalls that are configured and managed using industry best security practices.
- 5.2 Internal private Internet Protocol (IP) addresses must not be publicly accessible or natively routed to the Internet. Network address translation (NAT) technology should be used.
- 5.3 Administrative access to Firewalls and servers must be performed through a secure internal wired connection only.
- 5.4 Any standalone computers that directly access the Internet must have a desktop Firewall deployed that is installed and configured to block unnecessary/unused ports, services and network traffic.
- 5.5 Encrypt Wireless access points with a minimum of WEP 128 bit encryption, WPA encryption where available.
- 5.6 Disable vendor default passwords, SSIDs and IP Addresses on Wireless access points and restrict authentication on the configuration of the access points.

### **6. Regularly Monitor and Test Networks**

- 6.1 Perform regular tests on information systems (port scanning, virus scanning, vulnerability scanning).
- 6.2 Use current best practices to protect your telecommunications system and any computer system or network device(s) you use to provide Services hereunder to access Data Facts, Inc. systems and networks. These controls should be selected and implemented to reduce the risk of infiltration, hacking, access penetration or exposure to an unauthorized third party by:
  - \* protecting against intrusions;
  - \* securing the computer systems and network devices;
  - \* and protecting against intrusions of operating systems or software.

**Record Retention:** *The Federal Equal Opportunities Act states that a creditor must preserve all written or recorded information connected with an application for 60 months. In keeping with the ECOA, Data Facts, Inc. requires that you retain the credit application and, if applicable, a purchase agreement for a period of not less than 60 months. When conducting an investigation, particularly following a breach or a consumer complaint that your company impermissibly accessed their credit report, Data Facts, Inc. will contact you and will request a copy of the original application signed by the consumer or, if applicable, a copy of the sales contract.*

*"Under Section 621 (a) (2) (A) of the FCRA, any person that violates any of the provisions of the FCRA may be liable for a civil penalty of not more than \$2,500 per violation."*

Company Name: \_\_\_\_\_ Account #: \_\_\_\_\_

Company Representative: \_\_\_\_\_

Position/Title: \_\_\_\_\_

Date: \_\_\_\_\_

**All documents must be physically signed.**



## **BUSINESS INFORMATION SERVICES AGREEMENT**

This customer agreement is executed as of the date set forth below by the undersigned customer (hereinafter referred to as "Customer") for the benefit of Data Facts, Inc. (hereinafter referred to as "Reseller") and Experian Information Solutions, Inc. acting through its Business Information Solutions Group (hereinafter referred to as "Experian").

**A. Restrictions on Use.** In consideration for Customer's right to receive and use certain data and services on business entities (collectively, the "Services") from Reseller and Experian, Customer understands and certifies to Experian and Reseller that the Services:

- (i) Will be used solely in connection with a present or prospective credit or financial transaction with the business entity inquired upon or for other legitimate commercial purposes;
- (ii) Will not be used as a factor in establishing an individual's eligibility for (a) credit or insurance to be used primarily for personal, family or household purposes, or (b) employment;
- (iii) Will be used in compliance with all applicable laws, regulations and ordinances, and all special use restrictions set forth in the Agreement or adopted by Experian and/or Reseller hereafter; and
- (iv) Will be maintained in confidence and disclosed only to persons whose duties reasonable relate to the business purposes for which the information was request.
- (v) Will not be resold to any third party.

**B. Additional Restrictions for Business Owner Profile or Small Business Intelliscore or any other Experian or Reseller Service containing consumer credit information.**

- (i) is the proprietor of an unincorporated business;
- (ii) is a general partner in a partnership;
- (iii) is a guarantor of the business' obligation and has provided a copy of a written guaranty; or
- (iv) has given written instruction for the provision of such information;
- (v) will be used solely as an account monitoring tool when Experian Portfolio Monitoring Services are being provided;
- (vi) will be used in compliance with all applicable laws, regulations and ordinances, and all special use restrictions set forth in any agreement with Customer, Reseller and Experian or adopted by Experian or Reseller hereafter; and
- (vii) will be maintained in confidence and disclosed only to persons whose duties reasonably relate to the business purposes for which the information was requested.



- (viii) Customer understands that consumer data is not offered or permitted, and no access is granted to these services by Experian or Reseller under this agreement.

Every inquiry made on an individual will appear on such individual's Experian Consumer Information Solutions Group consumer credit report, listed as a BOP, SBI or account monitoring inquiry when using these reports, and will include the customer's business name and address.

**C. Terms and Conditions:** Customer agrees:

- (i) This agreement shall be in effect for one (1) year from the date hereunder and thereafter shall be automatic for additional (1) year periods, unless either party notifies the other in writing at least thirty (30) days prior to a current expiration date.
- (ii) That payment for these services shall be remitted to Data Facts, Inc. no more than thirty (30) days from receipt of each invoice unless other terms are agreed upon by an Officer of Data Facts, Inc. in writing. It is further agreed that if payment is not received within this designated time frame, Data Facts, Inc. may impose a late fee or finance charge of not more than 1.5% of the outstanding balance due. Should this account become more than sixty (60) days delinquent, Customer further agrees to pay any and all fees, including reasonable attorney fees and court costs, which may be incurred in the collection of this account.
- (iii) Customer is responsible for payment of the entire subscription fee unless Data Facts and Experian agree to new terms. If at any point the customer needs to cancel the contract, they will be required to pay the remainder of the subscription fee in full.
- (iv) That this agreement shall be governed by the laws of the State of Tennessee, without regard to conflicts of law principles.

**D. Warranty Disclaimer and Limitation of Liability.** Customer further acknowledges and agrees that the data and services:

- (i) are not guaranteed and that neither Experian, Reseller nor their collective sources, officers, employees, independent contractors nor agents will be liable to the Customer for any loss or damage based on any errors or omissions there from;
- (ii) are subject to the following exclusion of warranty. EXPERIAN, RESELLER AND THEIR COLLECTIVE SOURCES DO NOT GUARANTEE OR WARRANT THE ACCURACY, COMPLETENESS, CURRENTNESS, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OF THE SERVICES, DATA OR THE MEDIA ON WHICH THE DATA IS PROVIDED AND SHALL NOT BE LIABLE TO CUSTOMER FOR ANY LOSS OR INJURY ARISING OUT OF OR CAUSED IN WHOLE OR IN PART BY RESELLER'S, EXPERIAN'S OR THEIR COLLECTIVE SOURCES' ACTS OR OMISSIONS, WHETHER NEGLIGENT OR OTHERWISE, IN PROCURING, COMPILING, COLLECTING, INTERPRETING, REPORTING, COMMUNICATING OR DELIVERY THE DATA OR SERVICES. IN NO EVENT SHALL RESELLER, EXPERIAN OR THEIR COLLECTIVE SOURCES BE LIABLE TO CUSTOMER OR ANY THIRD PARTY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL OR SPECIAL DAMAGES (INCLUDING BUT NOT LIMITED TO DAMAGES TO BUSINESS REPUTATION, LOST BUSINESS OR LOST PROFITS), WHETHER FORESEEABLE OR NOT, AND

HOWEVER CAUSED, EVEN IF RESELLER, EXPERIAN OR THEIR COLLECTIVE SOURCES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS PARAGRAPH STATES RESELLER'S, EXPERIAN'S AND THEIR COLLECTIVE SOURCES' ENTIRE LIABILITY AND THE SOLE REMEDY OF CUSTOMER IN CONNECTION WITH THE PROVISION OF THE DATA AND SERVICES.

- (iii) IF, NOTWITHSTANDING THE PRIOR PARAGRAPH, LIABILITY CAN BE IMPOSED ON RESELLER, EXPERIAN OR THEIR COLLECTIVE SOURCES, THEN CUSTOMER AGREES THAT THE AGGREGATE LIABILITY FOR ANY OR ALL LOSSES OR INJURIES TO CUSTOMER CONNECTION WITH ANYTHING TO BE DONE OR FURNISHED UNDER THE AGREEMENT, REGARDLESS OF THE CAUSE OR THE LOSS OR INJURY (INCLUDING NEGLIGENCE) AND REGARDLESS OF THE NATURE OF THE LEGAL OR EQUITABLE RIGHT CLAIMED TO HAVE BEEN VIOLATED, SHALL NEVER EXCEED THE AMOUNT PAID TO RESELLER FOR THE AFFECTED SERVICES AND CUSTOMER COVENANTS AND PROMISES THAT IT WILL NOT SUE RESELLER, EXPERIAN OR THEIR COLLECTIVE SOURCES FOR AN AMOUNT GREATER THAN SUCH SUM AND THAT IT WILL NOT SEEK PUNITIVE DAMAGES IN ANY SUIT AGAINST RESELLER, EXPERIAN OR THEIR COLLECTIVE SOURCES.

**BUSINESS INFORMATION SERVICES AGREEMENT  
SIGNATURE PAGE**

**Name of Customer:** \_\_\_\_\_

**Signature:** \_\_\_\_\_

**Print Name:** \_\_\_\_\_

**Title:** \_\_\_\_\_

**Date:** \_\_\_\_\_

**Data Facts, Inc.**

**Signature:** \_\_\_\_\_

**Print Name:** \_\_\_\_\_

**Title:** \_\_\_\_\_

**Date:** \_\_\_\_\_





## Membership Application

Date :

Representative:

Company Name:

Type of Ownership (indicate one) ☐ Partnership ☐ Sole Owner ☐ Nonprofit ☐ Corporation ☐ LLC

Physical Address:

Mailing Address (if different)

City, State, Zip:

How long?      Years      Months

Company Phone:

Contact Phone

Fax:

Email:

Federal Tax ID.

What is the nature of your business:

How long has your company been in business:

Type of Report	#of Reports	Amount

☐ My Company agrees to submit our accounts receivable information electronically to Data Facts, Inc. and Experian on a ☐ monthly, ☐ quarterly basis.

Your authorized signature below is acknowledgement that the above Preferred Customer rates are contingent upon your payment of the agreement within 30 days of the signature.

\_\_\_\_\_ this day \_\_\_\_\_ month \_\_\_\_\_ year \_\_\_\_\_

DFI Representative:

Start Date:

8520 Macon Road, Suite 2 • Cordova, Tennessee 38018

www.datafacts.com • (901) 685-7599 • (800) 264-4110 • fax (901) 685-5013