American Financial Management

Experian Business Information Products

This Business Information Services Agreement (the "Agreement") is entered into by American Financial Management, Inc. (referred herein as "AFM"), an Illinois corporation, acting as reseller of Experian Business Information Solutions, Inc. (referred herein as "Experian") and the subscriber identified below at the signature line (referred to herein as "you" or "your"). You and American Financial Management, Inc., as reseller of Experian, agree as follows:

1. **Experian Services.** AFM will provide Experian business credit services (the "Experian Services") to you on the terms and conditions set forth herein. This Agreement and your right to use the information provided via the Experian Services is conditioned upon your acceptance of such terms and conditions.

2. **Grant of Right.** AFM, as reseller of Experian, grants you the right to use the information obtained through Experian Services for your internal use in connection with a business credit or risk management transaction, and not for resale, transfer or redistribution to third parties. AFM's written permission is required before any portion of this information may be copied or otherwise disseminated to third parties. Experian reserves all right, title and interest in the information provided via the Experian Services, which is protected under United States copyright laws.

3. **Effective Date.** This Agreement is not effective until executed and you are issued an Experian subscriber number.

4. **Rescission.** If AFM rescinds this Agreement, you will be billed for any usage of the Experian Services prior to rescission.

5. **Term.** The term of this Agreement ("Term") shall be the period beginning on the effective date (Item #3, above) and ending on the earliest of the following end dates (i) one year, (ii) when you have purchased Experian Services under this Agreement equal to or exceeding the Contract Amount indicated in Item #9, below, or (iii) until this Agreement is terminated pursuant to section 8. If this Agreement expires without renewal, your usage of Experian Services thereafter will be at the discretion of AFM and you will be charged at the prevailing non-subscriber rates.

6. **Renewal.** If you and AFM agree to renew this Agreement within thirty (30) days of expiration, then AFM will adjust your charges for the post-expiration, pre-renewal period to reflect the rates set forth in your renewal Agreement. Each renewal is subject to the "Term" provisions in 5 above. A renewal may occur without signing a new Agreement.

7. **Carryover.** If, after one year, you have not exhausted your Contract amount, you will not be entitled to a refund of any prepaid amounts. However, if you renew your Agreement within thirty (30) days of its expiration, and the Contract Amount of the renewal agreement exceeds $1,000, you may carryover one hundred percent (100%) of the unexhausted contract amount. **This provision does not apply to Subscription Plans.**

8. **Termination.** AFM may terminate this Agreement for default if you fail to make payments as required in the Agreement or if you breach any terms of the Agreement. Termination will not release you from any obligation arising prior to the effective date of the termination.

9. **Prices and Charges.** You agree to pay the fees and charges for Experian Services in accordance with the Price Schedule. This Price Schedule is adjusted annually to reflect current Experian pricing. All prices and fees are exclusive of applicable taxes and duties, and you agree to be responsible for all such taxes and duties. Applicable state and local taxes will be charged upon usage of the Experian Services and applies as contract usage. **Contract Amount**_____ **Initials**_____

10. **Invoicing and Payment.** Payment is due upon receipt of AFM'S invoice, and will be considered delinquent if payment is not received by AFM within thirty (30) days of the invoice date. AFM reserves the right to add a late charge to all delinquent amounts at the rate of one and onehalf percent (1.5%) per month or the highest legal rate. If you exhaust your Contract Amount prior to the Agreement end date, and any portion of the Contract Amount has not been billed, you will be invoiced for the unbilled Contract Amount, which is due upon receipt. AFM will provide you with a monthly usage statement reflecting your usage of Experian Services and the amounts charged against the Contract Amount.

11. **Proprietor Information-Certification.** You hereby certify that you will use the consumer credit information provided to you by Experian's Consumer Information Solutions Division in the Experian Business Owner Profile and Experian Blended Intelliscore Plus (previously Small Business Intelliscore) solely in connection with a commercial (i.e. not for personal, family or household purposes) credit transaction involving the individual on whom such information is sought, and only if the individual (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 to you a copy of such written guaranty); or (iv) has given written instruction for the provision of such information. Every inquiry you make on an individual will appear on such individual's Experian Information Solutions Division consumer credit report, listed as Experian's Business Owner Profile inquiry, and will include your business name.

American
Financial
Management

12. **Subscriber Warranties and Indemnities.** You warrant to AFM/Experian that you will request and use the Experian Services to be provided pursuant to this Agreement solely for the purpose of evaluating actual or contemplated business transactions involving the business entity to which the information relates. You further warrant that your use of the Experian Services described in this Agreement shall comply with all applicable federal, state, and local laws, statutes and regulations and Experian use regulations. Except as required by law, you agree not to divulge, sell or transfer the information provided via the Experian Services to any third party without AFM's prior written consent. You agree

13. to defend, indemnify and hold AFM/Experian harmless against all third-party claims resulting in or threatened to result in damages, loss or expense, including reasonable attorneys' fees, arising out of your use of the Experian Services provided under this Agreement.

14. **Subscriber Nondisclosure.** Except as required by law, you agree that all information obtained through the Experian Services will be maintained in strict confidence, will be disclosed only to those of your employees who have a legitimate need to know and will not be disclosed to any third parties. In the event that disclosure is required by law, you agree to provide AFM reasonable prior written notice of such disclosure.

15. **Exclusion of Warranty.** Because the Experian Services involve conveying information provided to Experian by other sources, Experian and AFM cannot and will not be an insurer or guarantor of the accuracy or reliability of the Experian Services. EXPERIAN AND AFM DO NOT
GUARANTEE OR WARRANT THE ACCURACY, COMPLETENESS, CURRENTNESS, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OF THE EXPERIAN SERVICES, THE INFORMATION IN THE EXPERIAN SERVICES OR THE MEDIA ON WHICH THE INFORMATION IS PROVIDED.

Signature Required On Reverse Side

15. **Limitation of Liability.** You understand and acknowledge that Experian maintains a database, updated on a periodic basis, from which you solicit information, and that Experian does not undertake a separate investigation for each inquiry you make. In addition, you acknowledge that the prices charged for Experian Services are based, in part, upon AFM's/Experian's expectation that the risk of any loss or injury that may be incurred by use of the Experian Services will be borne by you and not AFM/Experian. Therefore, you agree to be responsible for determining that the Experian Services provided hereunder are in accordance with AFM's /Experian's obligations to you. If you reasonably determine that the Experian Services are not so provided, following your receipt and inspection thereof, you will so notify AFM in writing within ten (10) days after receipt of the applicable Experian Services. Your failure to so notify AFM will mean that you accept the Experian Services as is, and AFM shall have no liability whatsoever for such Services. If you do so notify AFM, unless AFM disputes your claim, AFM shall, at its option, either reperform the applicable Services or issue you a credit for the amount you paid for the nonconforming Services. Such re-performance or credit shall constitute your sole remedy and AFM's maximum liability for any breach of this Agreement. AFM/EXPERIAN SHALL NOT BE LIABLE TO YOU FOR ANY LOSS OR INJURY ARISING OUT OF OR CAUSED IN WHOLE OR IN PART BY ACTS OR OMISSIONS, WHETHER NEGLIGENT OR OTHERWISE, IN PROCURING, COMPILING, COLLECTING, INTERPRETING, REPORTING, COMMUNICATING OR DELIVERING THE EXPERIAN SERVICES OR IN OTHERWISE PERFORMING ITS OBLIGATIONS UNDER THIS AGREEMENT. IN NO EVENT SHALL AFM BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL OR SPECIAL DAMAGES, INCLUDING BUT NOT LIMITED TO DAMAGES TO BUSINESS, LOST BUSINESS, OR LOST PROFITS, WHETHER FORESEEABLE OR NOT AND HOWEVER CAUSED, EVEN IF AFM IS ADVISED OF SUCH POSSIBILITY OF DAMAGES.
If, notwithstanding the above, liability is imposed on AFM, then you agree that AFM's aggregate liability for any and all loss or injuries arising out of any acts of omissions of AFM in connection with anything to be done or furnished under this Agreement, regardless of the cause of the loss or injury and regardless of the nature of the legal or equitable right claimed to have been violated, shall not exceed the lesser of the amount paid by you under this Agreement or Five Thousand Dollars ($5,000). You agree that you will not sue AFM for an amount greater than such sum and that you will not seek punitive damages in any suit against AFM.

16. **Excusable Delays.** Neither party shall be liable for any delay or failure in its performance under this Agreement (other than for payment obligations hereunder) if and to the extent that such delay or failure is caused by events beyond the reasonable control of the party including, without limitation, acts of God or public enemies, labor disputes, equipment malfunctions, computer downtime, software defects, material or component shortages, supplier failures, embargoes, rationing, acts of local, state or national government or public agencies, utility or communication failures or delays, fire, earthquakes, flood, epidemics, riots, strikes.

17. **Binding Arbitration.** With the exception of any action taken under Sections 2,9,10,11,12,13,16 or 17, the parties will resolve any dispute arising out of or relating to this Agreement, or the parties' respective rights hereunder, in a binding arbitration conducted under the auspices of the American Arbitration Association. Disputes arising out of or resulting from any action taken under Section 2,9,10,11,12,13,16 and 17 of this Agreement may be resolved by an action at law in equity. The prevailing party in any arbitration or action shall be entitled to an award of its reasonable attorney's fees and costs.

American
Financial
Management

18. **Choice of Law.** This Agreement will be governed in accordance with the procedural and substantive laws of the State of Illinois, without regard to any conflicts of laws provision. Any legal action will be initiated within the state of Illinois.

19. **Savings Clause.** This Agreement shall be deemed to be severable, and if any provision to be void or unenforceable, then such provision will be deemed severed and the remainder of the Agreement shall be enforced.

20. **Entire Agreement.** This Agreement sets forth the entire understanding and agreement of the parties and supersedes all other agreements, communications or understandings, whether written or oral. This Agreement may not be modified except by written amendment signed by authorized representatives of both parties.

21. You _____will _____will not contribute data to Experian. **IF YES or ALREADY CONTRIBUTE, the Contributor Addendum shall be incorporated into this Agreement by reference.**

IN WITNESS HEREOF, the subscriber has executed this Agreement on _____.
Date

_____
Company Name of Subscriber – Print or Type

_____ _____
Signature Address

_____ _____
Name of Signer – Print or Type City/State Zip Code

_____ _____
Title of Signer – Print or Type Telephone Number

_____ _____
Name of Primary Contact at Customer Site Fax Number

American Financial Management, Inc.
A Reseller Of Experian Information Solutions, Inc.

_____
Assigned Subscriber Number

8/16

Agreement / Application

This Agreement, dated _____ is made between American Financial Management, Inc., an Illinois corporation, as a reseller of Experian Information Solutions, and applicant, in order to obtain access to the Experian consumer database. **All information must be completed in its entirety.**

General Company Information

Company Name: _____ Years In Business _____ yrs. _____ mos.
Type of Ownership (Circle One): Partnership Sole Owner Nonprofit Corporation LLC
Do you have any other company names or dba? Yes No
If yes, please list _____
Physical Street Address (no P.O. Box Numbers, Please): _____
City: _____ State: _____ ZIP: _____ How Long? _____yrs._____mos._____
Phone: ( ) _____ Fax: ( ) _____ Is this a residential address? Yes No
If less than 2 years, indicate previous address: _____
City: _____ State: _____ ZIP: _____ How Long? _____yrs._____mos._____

Principal of the Company (If sole owner or partnership, please complete the section below.)

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 on accepting this application.
Principal name: _____
Title or Position: _____ Phone: ( ) _____
Social Security Number: _____ Year of Birth: _____
Residential Street Address: _____
City: _____ State: _____ ZIP: _____

Business Information

Type of Business: _____ Do you need a Purchase Order? Yes No
Do you have any branch offices located in the state of California? Yes No
Bank Reference (Please provide the name of the bank which maintains your business banking account.)
Bank Name: _____ Phone: ( ) _____
Address: _____
City: _____ State: _____ ZIP: _____
Business Checking Account Number(s): _____

Permissible Purpose / Appropriate Use **(This Section Must Be Completed)**

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

_____
_____
_____
_____

You may only access Experian information for the purpose(s) indicated above. Changes to this Agreement must be in written form and executed by both parties to this Agreement.

Security Designate Authorization Form

This form is to be used by Subscribers to identify the individual(s) designated to act on behalf of the Subscriber with regard to submission of requests to add, change or remove end user access accounts and permissions to systems and information. Designees must be employees of the Subscriber and must be able to interact with Security Administration, when needed, on security matters, in accordance with your Information Security Policy. Designate authorization forms will not be accepted unless signed by a duly authorized Subscriber officer. Changes in Security Designate status (e.g. transfer or termination) are to be reported to Security Administration immediately. Change requests must be faxed to both Experian Security Administration at 714-830-2403 and to American Financial Management at 847-259-7014.

SUBSCRIBER HEAD DESIGNATE INFORMATION

Company Name:		Phone:		Fax:	
Street Address:		City State:		Zip Code:	
Head Designate Name:		Title:		Phone:	
Designate Location: (If other than Company Address)		City State:		Zip Code:	
E-mail Address:					
Subcode					

SUBSCRIBER BACKUP DESIGNATE INFORMATION (Optional)

1) Backup Designate Name:		Title:		Phone:	
Backup Designate Location: (If other than Company Address)		City State:		Zip Code:	
E-mail Address:					
2) Backup Designate Name:		Title:		Phone:	
Backup Designate Location: (If other than Company Address)		City State:		Zip Code:	
E-mail Address:					
Comments:					
Authorized Officer: (Print)		Title:		Phone:	
Approval Signature:				Date:	

FOR AFM INTERNAL USE ONLY (Do Not Write Below This Line)

Date Received:		Reviewed By:		Subcode:	
Comments:					

Security Designate Roles and Responsibilities Agreement

The Security Designate is the individual the customer authorizes to act on behalf of the business in regards to Experian product access control (e.g. request to add/change/remove Internet access). A Company can opt to appoint more than one designate (e.g. for backup). The customer should understand that the designate(s) it appoints must be someone who will be available (Business hours 8am-5pm) and can liaison with addition or on information and product access matters.

The Security Designate:

1. Must be a duly appointed representative of Subscriber's company, identified as an approval point for Subscriber's Authorized Users.
2. Is responsible for the initial and on-going authentication and validation of Subscriber's Authorized Users and must maintain current information about each (phone number, valid email address, etc.).
3. Must notify AFM to add, change, and lock users within Subscriber's company, if no Experian automated facilities have been provided.
4. Is responsible for ensuring that proper privileges and permissions have been granted in alignment with Authorized User's job responsibilities.
5. Must ensure that standard security administration functions are performed within Subscriber's company. These include periodic review of Authorized User's activities, Authorized User's access rights, inactivity reviews, authentication and authorization process review, etc.
6. Is responsible for ensuring that Subscriber's Authorized Users are authorized to access Experian products and services.
7. Must disable Authorized User ID if it becomes compromised or if the Authorized User's employment is terminated by Subscriber.
8. Ensure password and ID records remain secure in Subscriber's environment and are issued to and shared only with the appropriate Authorized User.
9. Must advise Authorized Users not to share/post password or ID information.
10. Must advise Authorized Users of their responsibility to access consumer information for specified business uses only.
11. Must advise Authorized Users not to leave their workstations unattended when accessing Experian products and services.
12. Must advise Authorized Users to secure any Experian provided or generated documentation.
13. Must immediately report any suspicious/questionable activity to AFM, as Reseller, regarding access to Experian products and services.
14. Must report any potential compromise of Subscriber's systems that may expose Experian/AFM provided products or data to security threats.
15. Must communicate to Authorized Users, the security practices and regularly audit compliance, within Subscriber's organization.
16. Must immediately report changes in Head Designate status (e.g. transfer or termination) to AFM/Experian Subscriber's duly authorized representative (e.g. contracting officer, security manager, etc.) must authorize changes to Subscriber Head Designate.
17. Will be informed of any inquiries about passwords or IDs requested of AFM by your Authorized Users.
18. Shall be available to interact with AFM when needed on matters of user access and authorization.

You will be informed of any inquiries about passwords or IDs made to AFM. AFM employees will not communicate ID or password information to any client employee, other than the security designate. Communication will be sent only to the security designate's validated email address. AFM and/or Experian reserves the right to audit the process employed and the documentation used to ensure your company's ID and password security. Any weakness or lack of documentation, as well as any user ID or password compromise will result in termination of company's access rights.

I have read and understand my responsibilities as Security Designate.

_____ _____

Company Name *Print Name*

NSG5

_____ _____ _____ _____

Subcode w/Preamble *Email Address* *Signature* *Date*

American Financial Management

EXPERIAN BUSINESS INFORMATION SOLUTIONS
PREPAID CONTRACT PRICE SCHEDULE
This price schedule is effective as of September 1, 2016. All prices are exclusive of taxes.

The Reports / Services indicated below represent those most frequently requested by subscribers. For other reports / services please call our client services department at (847) 259-7000 extension 117.

REPORT / SERVICE	PRICE
BUSINESS PROFILE REPORT *	**$ 35.00**
This comprehensive report provides a wealth of information to help make informed credit-granting decisions quickly and easily. Report highlights include current payment information, payment trending, public record information, legal public record search, UCC filings, company background information and Standard & Poor's financial information. **Public record information** includes Corporate Record Filings from 50 states, **Legal Public Record Search** Includes bankruptcies, liens, Judgments and UCC Searches.	
PREMIER PROFILE REPORT *	**$ 40.00**
In addition to everything included in the Business Profile Report, the Premier Profile Report includes a comprehensive view of a business's financial obligations as well as fraud screening, credit limit recommendation, additional background information on the business, a risk dashboard including predicting whether an account will file for bankruptcy, and more data elements than any other report.	
BUSINESS OWNER PROFILE *	**$ 15.75**
This report provides in-depth information on the proprietor's financial situation and is best used in conjunction with the Business Profile Report. Understanding how the proprietors handle their personal finances provides valuable insight on how they will likely handle their business finances. *Fair Credit Reporting Act (FCRA) and Gramm-Leach-Bliley (GLBA) regulations apply.*	
BUSINESS OWNER BACKGROUND REPORTS *	**$ 14.40**
The Business Owner Background Report℠ provides unprecedented visibility into a business principal's relationships with current and former business interests. Combining Experian's robust consumer and commercial assets with state-of-the-art analytics, the report provides a comprehensive evaluation of the fraud and credit risk associated with a business owner or principal.	
BUSINESS SUMMARY REPORT *	**$ 10.50**
This is a one-page report used for quick evaluation of low-balance transactions (generally less than $1,000). This allows you to match the appropriate credit assessment costs to the amount of the transaction risk.	
PUBLIC RECORD REPORTS *	
Experian's national public record database provides incremental public record details on the company you are researching.	
Corporate Record Search	**$ 16.00**
Fictitious Business Name/DBA Search	**$ 15.00**
Public Record Search (Bankruptcy, Liens, Judgments)	**$ 15.00**
UCC Search	**$ 19.00**
LIST OF SIMILARS FEE (Billed if no report pulled)	**$ 2.00**
ADMINISTRATIVE / FAX CHARGE (AFM pulls report)	**$ 6.00**
OVERUSAGE CHARGE (If Experian Renewal Contract is not received within 30 days of expiration) This is on a per report basis.	**$ 3.00**

* A $1.00 fee is charged on all searches.

Continued on next page

8755 West Higgins Road, Suite 610, Chicago, IL 60631
(800) 426-5532 | (847) 259-7000
www.afm-usa.com

American Financial Management

EXPERIAN BUSINESS INFORMATION SOLUTIONS
PREPAID CONTRACT PRICE SCHEDULE (continued…)
This price schedule is effective September 1, 2016. All prices are exclusive of taxes.

REPORT / SERVICE	PRICE
COMMERCIAL INTELLISCORE PLUS℠ *	**$ 18.50**
This one-page statistical report uses past payment behavior to predict the likelihood of an account becoming delinquent. The report includes a summary of business information, key determining score factors and a score.	
BLENDED INTELLISCORE PLUS℠ * (previously, SMALL BUSINESS INTELLISCORE℠ *)	**$ 22.00**
This one-page statistical score report integrates both the business' and the business owner's credit history. Studies have shown that for small businesses, combined business and consumer data give a more complete representation of risk. *FCRA and GLBA regulations apply.*	
EXPERIAN'S SCORE-ONLY *	
These reports use the same statistical scoring model as in the full report but do not contain data element details such as trade account balances, days beyond terms or public record.	
Commercial Intelliscore Plus℠ *	**$ 13.50**
Blended Intelliscore Plus℠ * (previously, Small Business Intelliscore℠)	**$ 17.00**
COMBINATION REPORTS *	
This special pricing is available when reports are pulled simultaneously.	
Business Profile & Business Owner Profile	**$ 40.00**
Business Profile & Commercial Intelliscore Plus ℠	**$ 40.00**
Business Profile & Blended Intelliscore Plus ℠	**$ 40.00**
Business Owner Profile & Blended Intelliscore Plus ℠	**$ 32.00**
Business Profile & Business Owner Profile & Blended Intelliscore Plus ℠	**$ 45.00**
Premier Profile / Business Owner Profile	**$ 45.00**

* A $1.00 fee is charged on all searches.

Continued on next page

8755 West Higgins Road, Suite 610, Chicago, IL 60631
(800) 426-5532 | (847) 259-7000
www.afm-usa.com

American Financial Management

EXPERIAN BUSINESS INFORMATION SOLUTIONS
PREPAID CONTRACT PRICE SCHEDULE
This price schedule is effective September 1, 2016. All prices are exclusive of taxes.

REPORT / SERVICE	PRICE

INTERNATIONAL PROFILES **

Experian's International Profiles solution provides information on businesses in many countries around the world. These reports may be retrieved through online access or by requesting an International Developed Report.

ONLINE ACCESS

Online access to records in the United Kingdom provides you the information you need immediately. As additional countries go online, we will advise you.

United Kingdom Profile**	**$134.00**

Canadian reports may also be obtained online. However, American Financial will need to pull these reports for you and forward them to you. Please call 847-259-7000 extension 115.

Canadian Profile**	**$ 65.00**

INTERNATIONAL DEVELOPED PROFILES **

International Developed Profile reports are researched and written at the time of your order and are delivered to you based upon whether you select standard delivery – or priority delivery.

Western Europe (Priority Report – add $50.00)	**$155.00**
Scandinavia (Priority Report – add $60.00)	**$175.00**
Eastern Europe (Priority Report – add $60.00)	**$210.00**
Asia, China, Japan (Priority Report – add $70.00)	**$255.00**
Africa, Middle East (Priority Report – add $70.00)	**$255.00**
Australia & Pacific Island (Priority Report – add $70.00)	**$250.00**
Mexico, South America, Central America & Caribbean (Priority Report – add $60.00)	**$230.00**

Delivery Timeframe
Western Europe and Scandinavia – Standard Delivery is 4-7 Business Days;
Priority Delivery is 2-5 Business Days.
Rest of World - Standard Delivery is 7-10 Business Days;
Priority Delivery is 5-8 Business Days.

** A $3.00 fee is charged on all International Reports

Continued on next page

8755 West Higgins Road, Suite 610, Chicago, IL 60631
(800) 426-5532 | (847) 259-7000
www.afm-usa.com

American Financial Management

EXPERIAN BUSINESS INFORMATION SOLUTIONS
PREPAID CONTRACT PRICE SCHEDULE
This price schedule is effective September 1, 2016. All prices are exclusive of taxes.

Account Monitoring Services –

- **Portfolio Monitoring** is an online warning service that alerts you to significant changes on your commercial accounts. There is a flat fee charge per month for unlimited access to Portfolio Monitor Warning Detail Reports. Available via BizApps.
- **Account Monitoring Service** is a highly customizable customer monitoring service that notifies you of changes to the credit profile of your customers.

Portfolio Scoring –

- **Portfolio Scoring** is a batch process that offers clients consistent risk measurement criteria to evaluate their accounts receivable portfolio. When scoring is performed regularly, clients will be able to identify trends in accounts that are becoming more risky or that are becoming better credit risks.

Automated Decisioning –

- Through **DecisionIQ** Experian provides instant credit decisioning and prescreening based on a powerful combination of business and credit data and scores. Clients design matrices based upon risk categories, balance ranges, and commercial score ranges. These act as the foundation of the system which returns real-time information and client – specified credit policy instructions.

BizID –

- This commercial fraud product is intended to assess the fraud risk of small business applications by offering business and / or business owner verification and scoring, GLB and FCRA based product options, and flexible decisioning capabilities. This product draws on multiple Experian databases to identify potential fraud triggers on business and business principal application information. Reports can be purchased on the business only, on personal guarantors or both. Available via BizApps.

Business Collection Suite –

- A report that provides researching capabilities on business contacts, locations, telephone numbers and a 90 day cross trade payment summary.
- An online interface that allows the customer to segment their portfolio, and automatically execute letter campaigns informing clients of their delinquent status.

EXPERIAN BUSINESS INFORMATION SERVICES OFFERS ADDITIONAL SERVICES / REPORTS
Please call (847) 259-7000 extension 117 for additional information on these Services / Reports

American Financial Management

Important Experian Access Instructions and Inactivity Disclosures

All Experian Subscribers can pull Credit Reports on their customers through Experian's website. In order to do so, you need to login with your user id and password connected with your Experian sub code.

Please note that every Experian user must use his or her user id each month to keep the id active. If you do not need to pull a billable report in a given month, to keep your id active, please run a sample report for the customer described below. Experian will not bill your account for extracting this sample report.

Also, please note that this applies to each individual user id. Therefore, each user, individually, must pull the following sample report to keep his or her user id active if he or she does not need to pull a billable report in a particular month:

Crocker Industries 100
Main Street
Phoenix, AZ 85012

Experian will delete a sub code associated with a user id that is inactive for a six-month period. Thus, Experian will deny access to the inactive user id when an individual attempts to extract a report after that six-month inactive period.

Please contact Paulina Pashov at (847) 259-7000 x 117 with any questions.

American Financial Management

Experian™ A world of insight

Experian Canadian Credit Report Request

Request to pull a Canadian Credit Report through American Financial Management

Your Company Information:

Your Company Name:

Your Company Address:

Person Requesting Report:

Your E-Mail Address:

Date Submitted:

Business to Pull Report On:

Business Name:

Business Address:

City:

Province:

Postal Code:

Telephone Number:

Website:

Other related Information:

Please email or fax your request to Paulina Pashov at ppashov@afm-usa.com or (888) 800-6828.
Also, please contact Paulina at (847) 259-7000 x 217 if you have any questions.

Business Owner Profile/Small Business Intelliscore
Access Security Requirements

We must work together to protect the privacy of consumers. The following measures are designed to reduce unauthorized access of the consumer information contained in the Business Owner Profile and Small Business Intelliscore. In signing the Experian Membership Agreement, you agree to follow these measures.

1. You must protect your Experian account number and password so that only key personnel know this sensitive information. Unauthorized persons should never have knowledge of your password. Do not post the information in any manner within your facility.

2. System access software, whether developed by your company or purchased from a third party vendor, must have your Experian account number and password "hidden" or embedded and be known only by supervisory personnel. Assign each user of your system access software a unique logon password.

3. Do not discuss your Experian account number and passwords by telephone with any unknown caller, even if the caller claims to be an employee of Experian.

4. Restrict the ability to obtain credit information to a few key personnel.

5. Place all terminal devices used to obtain credit information in a secure location within your facility. You should secure these devices so that unauthorized persons cannot easily access them.

6. After normal business hours, be sure to turn off and lock all devices or systems used to obtain credit information.

7. Secure hard copies and electronic files of reports containing consumer information within your facility so that unauthorized persons cannot easily access them.

8. Shred or destroy all hard copy consumer reports when no longer needed.

9. Erase or scramble electronic files containing consumer information when no longer needed and when applicable regulation(s) permit destruction.

10. Make all employees aware that your company can access the Business Owner Profile and Small Business Intelliscore only for the permissible purposes listed in the Permissible Purpose Information section of your membership application. Your employees may not access their own report or the report of a family member or friend if your company does not have permissible purpose.

<u>Record Retention</u>: It is important that you keep credit applications for a reasonable period of time. This will help to facilitate the investigative process if a consumer claims that your company inappropriately accessed their credit report. (Note: The Federal Equal Credit opportunity Act states that a creditor must preserve all written or recorded information connected with an application for 25 months.)

"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."

FCRA Requirements

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

Although the FCRA primarily regulates the operations of consumer credit reporting agencies, it also affects you as a user of information. It is the position of the Federal Trade Commissions that the FCRA governs the use of the consumer data contained in the Business Owner Profile and Small Business Intelliscore. 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 Disclosures by Officers or Employees
621. Administrative Enforcement
623. Responsibilities of Furnishers of Information to Consumer Reporting Agencies

Each of these sections is of direct consequence to users who obtain the Business Owner Profile or Small Business Intelliscore.

Small Business Intelliscore and credit reports contained in the Business Owner Profile may be issued only if they are to be used in connection with a commercial (*i.e.*, not for personal, family or household purposes) credit transaction involving the individual on whom the information is being furnished and only if the individual (a) is the proprietor of an unincorporated business, (b) is a general partner in a partnership, (c) is a guarantor of the subject business obligation (and has provided to the customer a copy of such written guaranty), or (d) has given written instruction for the provision of such information.

Experian 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 statues and the statues and regulation of the states in which you operate.

We support consumer reporting legislation that will assure fair and equitable treatment for all consumers and users of credit information.

The FCRA, 15 U.S.C. 1681 et seq., is set forth in full at the Federal Trade Commissions' Internet web site (http://www.ftc.gov).

I have received, read and understand the **"FCRA Requirements"** notice and **"Access Security Requirements"** and will take all reasonable measures to enforce them within my facility / Company. I certify that I will use the Experian product information for no other purpose other than what is stated in the Permissible Purpose / Appropriate Use section of this Agreement / Application and for the type of business listed on this same Agreement / Application. I will not resell the report to any third party. I understand that if my system is used improperly by company personnel, or if my access codes are made available to any unauthorized personnel due to carelessness on the part of any employee of my company, I may be held responsible for financial losses, fees, or monetary charges that may be incurred and that my access privilege may be terminated.

I also acknowledge receipt of **"Notice To Users of Consumer Reports: Obligations of Users Under the FCRA".**

Important Tax Notice
If there is a reason for you to be exempt from state sales tax, please let us know in written form.

I certify that I have read the above statements and all information provided herein is accurate and hereby authorize the **Bank Reference to Release** information to either Experian or American Financial Management, Inc.

_____
Company Name

_____
Type or Print Name of Owner or Officer

_____
Authorized Signature

_____
Date

Access Security Requirements
for FCRA and GLB 5A Data

The following information security controls are required to reduce unauthorized access to consumer information. It is your (company provided access to Experian systems or data, referred to as the "Company") responsibility to implement these controls. If you do not understand these requirements or need assistance, it is your responsibility to get an outside service provider to assist you. Experian reserves the right to make changes to these Access Security Requirements without prior notification. The information provided herewith provides minimum baselines for information security.

In accessing Experian's services, Company agrees to follow these security requirements. These requirements are applicable to all systems and devices used to access, transmit, process, or store Experian data:

1. Implement Strong Access Control Measures

1.1 All credentials such as Subscriber Code number, Subscriber Code passwords, User names/identifiers (user IDs) and user passwords must be kept confidential and must not be disclosed to an unauthorized party. No one from Experian will ever contact you and request your credentials.

1.2 If using third party or proprietary system to access Experian's systems, ensure that the access must be preceded by authenticating users to the application and/or system (e.g. application based authentication, Active Directory, etc.) utilized for accessing Experian data/ systems.

1.3 If the third party or third party software or proprietary system or software, used to access Experian data/systems, is replaced or no longer in use, the passwords should be changed immediately.

1.4 Create a unique user ID for each user to enable individual authentication and accountability for access to Experian's infrastructure. Each user of the system access software must also have a unique logon password.

1.5 User IDs and passwords shall only be assigned to authorized individuals based on least privilege necessary to perform job responsibilities.

1.6 User IDs and passwords must not be shared, posted, or otherwise divulged in any manner.

1.7 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 eight (8) alphabetic and numeric characters for standard user accounts
- For interactive sessions (i.e. non system-to-system) ensure that passwords/passwords are changed periodically (every 90 days is recommended)

1.8 Passwords (e.g. subscriber code passwords, user password) must be changed immediately when:

- Any system access software is replaced by another system access software or is no longer used
- The hardware on which the software resides is upgraded, changed or disposed
- Any suspicion of password being disclosed to an unauthorized party (see section 4.3 for reporting requirements)

1.9 Ensure that passwords are not transmitted, displayed or stored in clear text; protect all end user (e.g. internal and external) passwords using, for example, encryption or a cryptographic hashing algorithm also known as "one-way" encryption. When using encryption, ensure that strong encryption algorithm are utilized (e.g. AES 256 or above).

1.10 Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations. Systems should be manually locked before being left unattended.

1.11 Active logins to credit information systems must be configured with a 30 minute inactive session timeout.

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 the membership application.

1.13 Company must NOT install Peer-to-Peer file sharing software on systems used to access, transmit or store Experian data.

1.14 Ensure that Company employees do not access their 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.

1.15 Implement a process to terminate access rights immediately for users who access Experian credit information when those users are terminated or when they have a change in their job tasks and no longer require access to that credit information.

1.16 Implement a process to perform periodic user account reviews to validate whether access is needed as well as the privileges assigned.

1.17 Implement a process to periodically review user activities and account usage, ensure the user activities are consistent with the individual job responsibility, business need, and in line with contractual obligations.

1.18 Implement physical security controls to prevent unauthorized entry to Company's facility and access to systems used to obtain credit information. Ensure that access is controlled with badge readers, other systems, or devices including authorized lock and key.

2. Maintain a Vulnerability Management Program

2.1 Keep operating system(s), firewalls, routers, servers, personal computers (laptops and desktops) and all other systems current with appropriate system patches and updates.

2.2 Configure infrastructure such as firewalls, routers, servers, tablets, smart phones, personal computers (laptops and desktops), and similar components to industry best security practices, including disabling unnecessary services or features, and 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 anti-virus software on all systems, if applicable anti-virus technology exists. Anti-virus software deployed must be capable to detect, remove, and protect against all known types malicious software such as viruses, worms, spyware, adware, Trojans, and root-kits.
- Ensure that all anti-virus software is current, actively running, and generating audit logs; ensure that anti-virus software is enabled for automatic updates and performs scans on a regular basis.

- If you suspect an actual or potential virus infecting a system, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.

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 Experian data is classified Confidential and must be secured to in accordance with the requirements mentioned in this document 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 Experian data and information when stored electronically on any system including but not limited to laptops, tablets, personal computers, servers, databases using strong encryption such AES 256 or above.

3.5 Experian data must not be stored locally on smart tablets and smart phones such as iPads, iPhones, Android based devices, etc.

3.6 When using smart tablets or smart phones to access Experian data, ensure that such devices are protected via device pass-code.

3.7 Applications utilized to access Experian data via smart tablets or smart phones must protect data while in transmission such as SSL protection and/or use of VPN, etc.

3.8 Only open email attachments and links from trusted sources and after verifying legitimacy.

3.9 When no longer in use, ensure that hard-copy materials containing Experian data are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.

3.10 When no longer in use, electronic media containing Experian data is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).

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 Safeguards Rule.

4.2 Suitable to complexity and size of the organization, establish and publish information security and acceptable user policies identifying user responsibilities and addressing requirements in line with this document and applicable laws and regulations.

4.3 Establish processes and procedures for responding to security violations, unusual or suspicious events and similar incidents to limit damage or unauthorized access to information assets and to permit identification and prosecution of violators. *If you believe Experian data may have been compromised, immediately notify Experian within twenty-four (24) hours or per agreed contractual notification timeline (See also Section 8).*

4.4 The FACTA Disposal Rules requires that Company 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.

4.5 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security in the organization.

4.6 When using third party service providers (e.g. application service providers) to access, transmit, store or process Experian data, ensure that service provider is compliant with

Experian Independent Third Party Assessment (EI3PA) program, and registered in Experian list of compliant service providers. If the service provider is in process of becoming compliant, it is Company responsibility to ensure the service provider is engaged with Experian and exception is granted in writing. *Approved certifications in lieu of EI3PA can be found in the Glossary section.*

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 stand-alone 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 Change vendor defaults including but not limited to passwords, encryption keys, SNMP strings, and any other vendor defaults.

5.6 For wireless networks connected to or used for accessing or transmission of Experian data, ensure that networks are configured and firmware on wireless devices updated to support strong encryption (for example, IEEE 802.11i) for authentication and transmission over wireless networks.

5.7 When using service providers (e.g. software providers) to access Experian systems, access to third party tools/services must require multi-factor authentication.

6. Regularly Monitor and Test Networks

6.1 Perform regular tests on information systems (port scanning, virus scanning, internal/ external vulnerability scanning). Ensure that issues identified via testing are remediated according to the issue severity (e.g. fix critical issues immediately, high severity in 15 days, etc.)

6.2 Ensure that audit trails are enabled and active for systems and applications used to access, store, process, or transmit Experian data; establish a process for linking all access to such systems and applications. Ensure that security policies and procedures are in place to review security logs on daily or weekly basis and that follow-up to exceptions is required.

6.3 Use current best practices to protect telecommunications systems and any computer system or network device(s) used to provide Services hereunder to access Experian 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.

7. Mobile and Cloud Technology

7.1 Storing Experian data on mobile devices is prohibited. Any exceptions must be obtained from Experian in writing; additional security requirements will apply.

7.2 Mobile applications development must follow industry known secure software development standard practices such as OWASP and OWASP Mobile Security Project adhering to common controls and addressing top risks.

7.3 Mobile applications development processes must follow secure software assessment methodology which includes appropriate application security testing (for example: static, dynamic analysis, penetration testing) and ensuring vulnerabilities are remediated. Mobility

7.4 solution server/system should be hardened in accordance with industry and vendor best practices such as Center for Internet Security (CIS) benchmarks, NIS, NSA, DISA and/or other. Mobile applications and data shall be hosted on devices through a secure container separate

7.5 from any personal applications and data. See details below. Under no circumstances is Experian data to be exchanged between secured and non-secured applications on the mobile device.

In case of non-consumer access, that is, commercial/business-to-business (B2B) users

7.6 accessing Experian data via mobile applications (internally developed or using a third party application), ensure that multi-factor authentication and/or adaptive/risk-based authentication mechanisms are utilized to authenticate users to application.

When using cloud providers to access, transmit, store, or process Experian data ensure that:

7.7

- Appropriate due diligence is conducted to maintain compliance with applicable laws and regulations and contractual obligations
- Cloud providers must have gone through independent audits and are compliant with one or more of the following standards, or a current equivalent as approved/recognized by Experian:
  - ISO 27001
  - PCI DSS
  - EI3PA
  - SSAE 16 – SOC 2 or SOC3
  - FISMA
  - CAI / CCM assessment

8. **General**

8.1 Experian may from time to time audit the security mechanisms Company maintains to safeguard access to Experian information, systems and electronic communications. Audits may include examination of systems security and associated administrative practices

8.2 In cases where the Company is accessing Experian information and systems via third party software, the Company agrees to make available to Experian upon request, audit trail information and management reports generated by the vendor software, regarding Company individual Authorized Users.

8.3 Company shall be responsible for and ensure that third party software, which accesses Experian information systems, is secure, and protects this vendor software against unauthorized modification, copy and placement on systems which have not been authorized for its use.

8.4 Company shall conduct software development (for software which accesses Experian information systems; this applies to both in-house or outsourced software development) based on the following requirements:

8.4.1 Software development must follow industry known secure software development standard practices such as OWASP adhering to common controls and addressing top risks.

8.4.2 Software development processes must follow secure software assessment methodology which includes appropriate application security testing (for example:

static, dynamic analysis, penetration testing) and ensuring vulnerabilities are remediated.

8.4.3 Software solution server/system should be hardened in accordance with industry and vendor best practices such as Center for Internet Security (CIS) benchmarks, NIS, NSA, DISA and/or other.

8.5 Reasonable access to audit trail reports of systems utilized to access Experian systems shall be made available to Experian upon request, for example during breach investigation or while performing audits

8.6 Data requests from Company to Experian must include the IP address of the device from which the request originated (i.e., the requesting client's IP address), where applicable.

8.7 Company shall report actual security violations or incidents that impact Experian to Experian within twenty-four (24) hours or per agreed contractual notification timeline. Company agrees to provide notice to Experian of any confirmed security breach that may involve data related to the contractual relationship, to the extent required under and in compliance with applicable law. Telephone notification is preferred at 800-295-4305, Email notification will be sent to regulatorycompliance@experian.com .

8.8 Company acknowledges and agrees that the Company (a) has received a copy of these requirements, (b) has read and understands Company's obligations described in the requirements, (c) will communicate the contents of the applicable requirements contained herein, and any subsequent updates hereto, to all employees that shall have access to Experian services, systems or data, and (d) will abide by the provisions of these requirements when accessing Experian data.

8.9 Company understands that its use of Experian networking and computing resources may be monitored and audited by Experian, without further notice.

8.10 Company acknowledges and agrees that it is responsible for all activities of its employees/Authorized users, and for assuring that mechanisms to access Experian services or data are secure and in compliance with its membership agreement.

8.11 When using third party service providers to access, transmit, or store Experian data, additional documentation may be required by Experian.

Record Retention: The Federal Equal Credit Opportunity Act states that a creditor must preserve all written or recorded information connected with an application for 25 months. In keeping with the ECOA, Experian requires that you retain the credit application and, if applicable, a purchase agreement for a period of not less than 25 months. When conducting an investigation, particularly following a consumer complaint that your company impermissibly accessed their credit report, Experian 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 $3,500 per violation."

Internet Delivery Security Requirements
In addition to the above, following requirements apply where Company and their employees or an authorized agent/s acting on behalf of the Company are provided access to Experian provided services via Internet ("Internet Access").

General requirements:

1. The Company shall designate in writing, an employee to be its Head Security Designate, to act as the primary interface with Experian on systems access related matters. The Company's Head Security Designate will be responsible for establishing, administering and monitoring all Company employees' access to Experian provided services which are delivered over the Internet ("Internet access"), or approving and establishing Security Designates to perform such functions.
2. The Company's Head Security Designate or Security Designate shall in turn review all employee requests for Internet access approval. The Head Security Designate or its Security Designate shall determine the appropriate access to each Experian product based upon the legitimate business needs of each employee. Experian shall reserve the right to terminate any accounts it deems a security threat to its systems and/or consumer data.
3. Unless automated means become available, the Company shall request employee's (Internet) user access via the Head Security Designate/Security Designate in writing, in the format approved by Experian. Those employees approved by the Head Security Designate or Security Designate for Internet access ("Authorized Users") will be individually assigned unique access identification accounts ("User ID") and passwords/passphrases (this also applies to the unique Server-to-Server access IDs and passwords/ passphrases). Experian's approval of requests for (Internet) access may be granted or withheld in its sole discretion. Experian may add to or change its requirements for granting (Internet) access to the services at any time (including, without limitation, the imposition of fees relating to (Internet) access upon reasonable notice to Company), and reserves the right to change passwords/passphrases and to revoke any authorizations previously granted. *Note: Partially completed forms and verbal requests will not be accepted.*
4. An officer of the Company agrees to notify Experian in writing immediately if it wishes to change or delete any employee as a Head Security Designate, Security Designate, or Authorized User; or if the identified Head Security Designate, Security Designate or Authorized User is terminated or otherwise loses his or her status as an Authorized User.

Roles and Responsibilities

1. Company agrees to identify an employee it has designated to act on its behalf as a primary interface with Experian on systems access related matters. This individual shall be identified as the "Head Security Designate." The Head Security Designate can further identify a Security Designate(s) to provide the day to day administration of the Authorized Users. Security Designate(s) must be an employee and a duly appointed representative of the Company and shall be available to interact with Experian on information and product access, in accordance with these Experian Access Security Requirements. The Head Security Designate Authorization Form must be signed by a duly authorized representative of the Company. Company's duly authorized representative (e.g. contracting officer, security manager, etc.) must authorize changes to Company's Head Security Designate. The Head Security Designate will submit all requests to create, change or lock Security Designate and/or Authorized User access accounts and permissions to Experian's systems and information (via the Internet). Changes in Head Security Designate status (e.g. transfer or termination) are to be reported to Experian immediately.

2. As a Client to Experian's products and services via the Internet, the Head Security Designate is acting as the duly authorized representative of Company.
3. The Security Designate may be appointed by the Head Security Designate as the individual that the Company authorizes to act on behalf of the business in regards to Experian product access control (e.g. request to add/change/remove access). The Company can opt to appoint more than one Security Designate (e.g. for backup purposes). The Company understands that the Security Designate(s) it appoints shall be someone who will generally be available during normal business hours and can liaise with Experian's Security Administration group on information and product access matters.
4. The Head Designate shall be responsible for notifying their corresponding Experian representative in a timely fashion of any Authorized User accounts (with their corresponding privileges and access to application and data) that are required to be terminated due to suspicion (or actual) threat of system compromise, unauthorized access to data and/or applications, or account inactivity.

Designate

1. Must be an employee and duly appointed representative of Company, identified as an approval point for Company's Authorized Users.
2. Is responsible for the initial and on-going authentication and validation of Company's Authorized Users and must maintain current information about each (phone number, valid email address, etc.).
3. Is responsible for ensuring that proper privileges and permissions have been granted in alignment with Authorized User's job responsibilities.
4. Is responsible for ensuring that Company's Authorized Users are authorized to access Experian products and services.
5. Must disable Authorized User ID if it becomes compromised or if the Authorized User's employment is terminated by Company.
6. Must immediately report any suspicious or questionable activity to Experian regarding access to Experian's products and services.
7. Shall immediately report changes in their Head Security Designate's status (e.g. transfer or termination) to Experian.
8. Will provide first level support for inquiries about passwords/passphrases or IDs requested by your Authorized Users.
9. Shall be available to interact with Experian when needed on any system or user related matters.

Experian

Glossary

Term	Definition
Computer Virus	A Computer Virus is a self-replicating computer program that alters the way a computer operates, without the knowledge of the user. A true virus replicates and executes itself. While viruses can be destructive by destroying data, for example, some viruses are benign or merely annoying.
Confidential	Very sensitive information. Disclosure could adversely impact your company.
Encryption	Encryption is the process of obscuring information to make it unreadable without special knowledge.
Firewall	In computer science, a Firewall is a piece of hardware and/or software which functions in a networked environment to prevent unauthorized external access and some communications forbidden by the security policy, analogous to the function of Firewalls in building construction. The ultimate goal is to provide controlled connectivity between zones of differing trust levels through the enforcement of a security policy and connectivity model based on the least privilege principle.
Information Lifecycle	(Or Data Lifecycle) is a management program that considers the value of the information being stored over a period of time, the cost of its storage, its need for availability for use by authorized users, and the period of time for which it must be retained.
IP Address	A unique number that devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP). Any All participating network devices - including routers, computers, time-servers, printers, Internet fax machines, and some telephones - must have its own unique IP address. Just as each street address and phone number uniquely identifies a building or telephone, an IP address can uniquely identify a specific computer or other network device on a network. It is important to keep your IP address secure as hackers can gain control of your devices and possibly launch an attack on other devices.
Peer-to-Peer	A type of communication found in a system that uses layered protocols. Peer-to-Peer networking is the protocol often used for reproducing and distributing music without permission.
Router	A Router is a computer networking device that forwards data packets across a network via routing. A Router acts as a junction between two or more networks transferring data packets.
Spyware	Spyware refers to a broad category of malicious software designed to intercept or take partial control of a computer's operation without the consent of that machine's owner or user. In simpler terms, spyware is a type of program that watches what users do with their computer and then sends that information over the internet.
Subscriber Code	Your seven digit Experian account number.
Experian Independent Third Party Assessment Program	The Experian Independent 3rd Party Assessment is an annual assessment of an Experian Reseller's ability to protect the information they purchase from Experian. EI3PA℠ requires an evaluation of a Reseller's information security by an independent assessor, based on requirements provided by Experian. EI3PA℠ also establishes quarterly scans of networks for vulnerabilities.
ISO 27001 /27002	IS 27001 is the specification for an ISMS, an Information Security Management System (it replaced the old BS7799-2 standard) The ISO 27002 standard is the rename of the ISO 17799 standard, and is a code of practice for information security. It basically outlines hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided

	within ISO 27001.
PCI DSS	The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.
SSAE 16 SOC 2, SOC3	Statement on Standards for Attestation Engagements (SSAE) No. 1 SOC 2 Report on Controls Related to Security, Availability, Processing Integrity, Confidentiality, and Privacy. The SOC 3 Report , just like SOC 2, is based upon the same controls as SOC 2, the difference being that a SOC 3 Report does not detail the testing performed (it is meant to be used as marketing material).
FISMA	The Federal Information Security Management Act (FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA was signed into law part of the Electronic Government Act of 2002.
CAI / CCM	Cloud Security Alliance Consensus Assessments Initiative (CAI) was launched to perform research, create tools and create industry partnerships to enable cloud computing assessments. The Cloud Security Alliance Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.

I _____ have received, read and understand the rules and guidelines of the Access Security Requirements for FCRA and GLB 5A Data. Furthermore, I agree to fully comply with all the rules and guidelines associated with Access Security Requirements for FCRA and GLB 5A Data and understand that at any time American Financial Management of Experian, may terminate my privileges due to non-compliance. This may include lack of proper paperwork submitted for access, or wrongful use of the services provided.

Signed,

_____

Full Name

_____

Job Title