Internet Access Request

experian

The Security Administration (SA) Group in Costa Mesa is responsible for processing all requests to establish Internet access accounts for Subscribers through Experian's existing E-Commerce applications. Please complete the following form in its entirety. Illegible and Incomplete forms will be sent back to the Requestor and will result in processing delays. For instructions on completing this form, please see your policy manual.

SALES CONTACT INFORMATION/CUSTOMER SECURITY DESIGNATE (Requestor)			
Name:	NACM Oregon	**Date of Request:**	
Location:	7931 NE Halsey, Suite 200 Portland, OR 97213	**Phone:**	971-230-1164
Manager:	Kathy Linscott	**Email:**	klinscott@nacmoregon.org
Have the original Addendum to the Subscriber Services Agreement for Internet Delivery, Security Designate Authorization Form, and Security Designate Roles and Responsibilities Agreement been received? ☐ Yes ☐ No			
Signature:			Date:

CUSTOMER CONTACT INFORMATION	
Company Name:	Subcode:
Customer Security Designate: Phone: Check if New ◯	
Title:	Email Address:

ACCESS (ES) REQUESTED FOR (Use attached list for more than 4 users)	
Employee Name:	
Title:	Phone:
Email Address: [1]	
Employee Name:	
Title:	Phone:
Email Address: [1]	
Employee Name:	
Title:	Phone:
Email Address: [1]	
Employee Name:	
Title:	Phone:
Email Address: [1]	

[1] Email addresses are required. Illegible, incomplete, or blank addresses will be returned to the requestor.

[1] Email addresses are required. Illegible, incomplete, or blank addresses will be returned to the requestor.

ADDITIONAL ACCESSES				
User ID	**Employee Name**	**Title**	**Phone**	**E-mail Address**

Security Designate Authorization Form

experian

This form is to be used by Experian 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 Experian systems and information. Designees must be employees of the Subscriber and must be available to interact with Experian Security Administration, when needed, on security matters, in accordance with Experian 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 Experian Security Administration immediately. For instructions on completing this form, please see your policy manual.

SUBSCRIBER DESIGNATE INFORMATION					
Company Name:		**Phone:**		**Fax:**	
Street Address:		**City State:**			
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:	**** GOOD TO HAVE A BACK UP DESIGNATE** **** PLEASE SIGN BELOW**				
Authorized Officer (Print):		**Title:**		**Phone:**	
Approval Signature:				**Date:**	

FOR EXPERIAN INTERNAL USE ONLY (Do Not Write Below This Line)					
Date Received:		**Reviewed By:**		**Subcode:**	
Comments:					

Addendum to Distributor's (or Experian's Direct Resellers) Business Information Services Agreement for Internet Delivery

This Addendum to Distributor's (or Experian's Direct Reseller's) Business Information Services Agreement for Internet Delivery (the "Addendum") is made as of _____, by and between **NACM Oregon** ("Distributor" or "Reseller"), **Experian Information Solutions, Inc.** ("Experian") and _____("Subscriber").

WHEREAS, Distributor (or Reseller) and Subscriber have entered into a Credit Report Agreement Terms and Conditions, dated _____ (the "Agreement") whereby Distributor (or Reseller) provides certain on-line business credit reporting services ("Services") to Subscriber; and

WHEREAS, Subscriber has requested access to certain services offered by Experian through an Internet connection ("Internet Credit Delivery Services" or "ICDS"), and Experian desires to allow such access based on Subscriber's and Distributor's (or Reseller's) agreement to the terms and conditions set forth herein.

NOW, THEREFORE, in consideration of the foregoing and other good and valuable consideration, Experian, Distributor (or Reseller) and Subscriber agree as follows:

1. Subscriber shall obtain Internet access to ICDS only through the individual Subscriber employees who are specifically approved by Experian upon the written request of Subscriber and on the terms and conditions contained in this Addendum (each an "Authorized Employee"). Subscriber shall request Internet access in writing in a form approved by Experian from time to time. Authorized Employees will be assigned unique access identification numbers ("User ID") and passwords. 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 ICDS at any time [including, without limitation, the imposition of fees relating to Internet Access upon reasonable notice to Distributor (or Reseller)], and reserves the right to change passwords and to revoke any authorizations previously granted. Distributor (or Reseller) shall notify Experian, in writing, whether or not Subscriber has signed a certification agreeing to comply with the federal Fair Credit Reporting Act relating to its use of Experian's Business Owner Profile ("BOP") and Small Business Intelliscore ("SBI") services. Subscriber may not access BOP or SBI services through an Internet connection unless such certification has been executed.

2. Only Authorized Employees shall utilize Internet access, and only through the User ID and password assigned to such employee by Experian. Subscriber shall request User ID's and passwords only for those employees of Subscriber who have a legitimate need to access ICDS in performing his or her duties for Subscriber. Prior to requesting User ID's for Authorized Employees, Subscriber shall provide adequate training regarding the requirements to this Addendum and applicable laws. Subscriber will ensure that each Authorized Employee (i) is familiar with the requirements specified herein, and agrees to comply with such requirements, (ii) agrees not to disclose the User ID and password assigned to the Authorized Employee to any other person, and (iii) agrees not to order business credit reports or other data from Experian's site except in performance of Employee's official duties for Subscriber.

3. Subscriber acknowledges and agrees that it is responsible for all activities of Subscriber's employees in utilizing Internet access and for assuring the facilities for receipt of information provided to it through the Internet are secure and in compliance with the Agreement. Subscriber shall not retransmit or otherwise make available to any person ICDS (including any of the information therein) on or through the Internet or other generally accessible network or delivery method.

4. Subscriber agrees to notify Experian in writing immediately if it wishes to delete any employee as an Authorized Employee or if any Authorized Employee is terminated or otherwise loses his or her status as an Authorized Employee.

5. Subscriber acknowledges and agrees that this Addendum is in addition to the requirements of Distributor's (or Reseller's) membership application process, including Access Security Requirements (except where expressly modified by this Addendum) which are applicable to Distributor's (or Reseller's) provision of BOP reports and SBI services. Subscriber will abide by any additional or further security procedures specified by Experian or Distributor (or Reseller) from time to time.

6. Subscriber shall use its best efforts to ensure the confidentiality of all User ID's and passwords issued by Experian to Subscriber's employees. Subscriber shall indemnify Experian against any damage or disruption to Experian systems or business caused by Subscriber's employees, subcontractors, subcontractor employees or its clients whether as a result of their access to such systems or compromise of password confidentiality or otherwise.

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

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

9. If Experian or Distributor (or Reseller) believes that Subscriber has breached a material obligation contained in this Addendum, Experian or Distributor (or Reseller) may terminate this Addendum immediately by providing the other parties notice of termination.

10. Experian shall have no obligation or liability for or on account of any mechanical or other breakdown, malfunction or defect in the Internet connection accessed by Subscriber. EXPERIAN MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, IN CONNECTION WITH THIS ADDENDUM. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, UNDER NO CIRCUMSTANCES WILL EXPERIAN HAVE ANY OBLIGATION OR LIABILITY TO SUBSCRIBER FOR ANY CLAIM, INJURY OR DAMAGE RELATING TO, ARISING OUT OF, OR RESULTING FROM SUBSCRIBER'S INTERNET ACCESS TO THE SERVICES.

11. NOTWITHSTANDING ANY OTHER PROVISION IN THIS AGREEMENT, UNDER NO CIRCUMSTANCES SHALL A PARTY BE LIABLE TO THE OTHER FOR ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL OR INDIRECT DAMAGES (INCLUDING, WITHOUT LIMITATION, ANY INDIRECT DAMAGES ARISING FROM THE LOSS OF BUSINESS, DATA, PROFITS OR GOODWILL WHICH ARE NOT DIRECT DAMAGES) INCURRED OR SUFFERED BY THAT PARTY BY REASON OF THE OTHER PARTY'S PERFORMANCE OR NONPERFORMANCE UNDER THIS ADDENDUM, OR FOR ANY OTHER REASON, EVEN IF APPRISED OF THE LIKELIHOOD OF SUCH DAMAGES.

12. Except as expressly amended by this Addendum, the Agreement remains in full force and effect. The terms of this Addendum shall prevail in the event of any inconsistency between this Addendum and the Agreement.

IN WITNESS WHEREOF, Subscriber, Distributor (or Reseller) and Experian have each caused this Addendum to be executed by their respective duly authorized representatives as of the date first above written.

Subscriber/NACM Oregon Member

Print or Type Name of Subscriber	Signature (Duly Authorized Officer Only)
Authorized Name (Print)	Title

Experian Information Solutions, Inc., by and through its Information Solutions Division

Experian Information Solutions Print or Type Name of Subscriber	Signature (Duly Authorized Officer Only)
Authorized Name (Print)	Title

NACM Affiliate

NACM Oregon Print or Type Name of Subscriber	Signature (Duly Authorized Officer Only)
Authorized Name (Print)	Title

Access Security Requirements
for FCRA and GLB 5A Data

We must work together to protect the privacy and information of consumers. The following information 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 get an outside service provider to assist you. Capitalized terms herein have the meaning given in the attached Glossary. Experian reserves the right to make changes to these Access Security Requirements without notification. The information provided herewith provides minimum baselines for information security.

In accessing Experian's services, you agree to follow these security requirements

1. <u>Implement Strong Access Control Measures</u>

1.1 Do not provide your Experian Subscriber Codes or passwords to anyone. No one from Experian will ever contact you and request your Subscriber Code number or password.

1.2 Proprietary or third party system software must have Experian Subscriber Codes and password(s) hidden. Account numbers and passwords 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 another system access software or is no longer used;
- The hardware on which the software resides is upgraded, changed or disposed.

1.4 Protect Experian Subscriber Code(s) and password(s) so that only key personnel know this information. Unauthorized personnel should not know your Subscriber Code(s) and password(s).

1.5 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.

1.6 Ensure that user IDs are not shared and that no Peer-to-Peer file 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 credit information systems 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 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.

1.15 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 (laptops and desktops) 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, 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 Computer Virus detection/scanning product on all computers, systems and networks.
- If you suspect an actual or potential virus, immediately cease accessing the 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 configuring auto updates and installing new virus definition files.

2.4 Implement and follow security best practices for computer anti-spyware scanning services and procedures:

- Use, implement and maintain a current, commercially available computer anti-spyware scanning product on computers, systems and networks.
- If you suspect actual or potential spyware, immediately cease accessing the system and do not resume the inquiry process until the problem has been resolved and 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-spyware software up-to-date by checking or configuring auto updates and installing new 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 Experian data is classified 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 Experian 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 Safeguards Rule.
4.2 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.
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 in 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 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 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 point.

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 systems and any computer system or network device(s) you use 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.

Record Retention: *The Federal Equal Credit Opportunity Act, Sec. 202.12, 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 $2,500 per violation."

I agree to implement and adhere to the above controls.

Company Name	Subcode
Authorized Name (Print)	Authorized Signature
Email Address	Date
1. Secondary Name (Print)	Signature
Email Address	Date
2. Secondary Name (Print)	Signature
Email Address	Date