



# BankersOnline.com

## Instructions:

For your convenience we've created this easy to follow checklist. Please provide all information requested in each section.

## SUBSCRIBER APPLICATION:

- Page 1 Company Information: Please complete all fields.
- Page 2 Company Details: Please complete all fields.
- Page 2 References: REQUIRED – please be sure to provide contact information for one bank and two trade references. A trade reference is any company you conduct business transactions with (customer, supplier, vendor, etc.).
- Page 3 Services: Please select your default background check package.
- Page 4 Services: Be sure this page is signed by an authorized company representative.

## USER AGREEMENT:

- All pages of the User Agreement and Exhibits A & B must be initialed at bottom left of page.
- User Agreement Page 1 paragraph 3: Please initial here to certify that you are utilizing our services for employment purposes.
- FAX OR SCAN/EMAIL ALL PAGES OF THE AGREEMENT TO (888) 390-4617. We will contact you shortly with screening documentation and next steps.

Questions? Contact John Sferry at (800) 235-3954 x 475



COMPANY INFORMATION – ALL FIELDS REQUIRED

Business Name

DBA (If Applicable)

Main Business Phone

Physical Address City State Zip

Billing Address (If Different) City State Zip

Main Contact Name Title Main Contact Email Address

Phone Fax

Additional Contact Name Title Email Address

Phone Fax

Additional Contact Name Title Email Address

Phone Fax

Billing Contact Name Title Email Address

Phone Fax

EmployeeScreenIQ Rep: John Sferry

## COMPANY DETAILS

Describe Your Type of Business:

\_\_\_\_\_

Business Type:  Sole Proprietor  Partnership  Corporation  Other: \_\_\_\_\_

Tax ID Number: \_\_\_\_\_

Please check all that apply:  Privately Held  Publicly Traded  Other: \_\_\_\_\_

Identify two principals (owners) of your business. Or if your company stock is traded on a recognized stock exchange please provide the symbol and exchange:

\_\_\_\_\_

Anticipated number of background checks per year: \_\_\_\_\_

Number of employees: \_\_\_\_\_

Are you an FDIC Insured Institution?  Yes  No

## REFERENCES

### Bank Reference

\_\_\_\_\_

Bank Name

Location

\_\_\_\_\_

Name on Account

Account Number

Contact Name

### Trade References

1. \_\_\_\_\_

Company Name

Contact Name

\_\_\_\_\_

Address

City

State

Zip

\_\_\_\_\_

Account Number

Phone

2. \_\_\_\_\_

Company Name

Contact Name

\_\_\_\_\_

Address

City

State

Zip

\_\_\_\_\_

Account Number

Phone

**A copy of your business license or an approved official federal document must accompany this agreement if you are not FDIC insured.**

## SERVICES

In the following section, please select the Package/s that you would like to be included as your default.

EmployeeScreenIQ is a Consumer Reporting Agency (CRA) as defined by the Fair Credit Reporting Act (FCRA). While we are structured to handle the needs of larger organizations, it is EmployeeScreenIQ policy to provide FCRA-compliant screening services for companies that do not have significant hiring activity.

We have created the following options for Bankers Online affiliated organizations:

**Basic Bankers Online Background Check: \$75.00**

- Social Security Number Trace
- Countywide Criminal Search (Includes all counties of residence and all alias names over the past 7 years)
- Federal District Criminal Record Search
- Homeland Security Check
- Financial Sanctions Check

**Mid Level Bankers Online Background Check: \$89.50**

- All Basic Package Services (Listed Above)
- Pre-Employment Credit Report
- Federal Bankruptcy Search

**Upper Management Bankers Online Background Check: \$139.50**

- All Basic & Mid Level Package Services (Listed Above)
- Education Verification
- 7-Year Unlimited Employment Verification

\*These packages cannot be altered in any way.

**\$125 Set Up Fee** – All new accounts are thoroughly vetted to ensure that the entities we are providing private and/or confidential information to are legitimate businesses with a permissible use for the information (employment screening is a permissible use under the FCRA). Please note that a Physical Inspection is required for all non-FDIC insured organizations.

**Research Fees – Please Note** there are various fees charged to EmployeeScreenIQ for access to different types of information. Because of the variability of these fees, we cannot build them into our price structure and must pass them along as incurred. There is never a profit margin built into any fees charged for access to information. Any fee added to a search is the direct cost of information as incurred by EmployeeScreenIQ.

### Examples are:

**County Court Access Fees** – less than 15% of approximately 10,000 court jurisdictions across the country charge an access fee, typically \$5.00-\$15.00. See Court Access Fee List below.

**New York Office of Court Administration** – approximately 16 counties in New York participate in the OCA program, which denies direct access to individual county criminal history records. Criminal history records in these counties are only accessible through the OCA, which charges \$65.00 for a “statewide” search. Counties currently accessible only through the OCA which will incur this fee are: Allegany, Bronx, Cayuga, Chemung, Cortland, Delaware, Fulton, Hamilton, Kings, Montgomery, Nassau, New York, Orleans, Putnam, Queens, and Richmond. The list of participating counties is subject to change.





Business Name \_\_\_\_\_

**1. DEFINITIONS**

For the purpose of this agreement “user” means the company, its employees and authorized representatives entering into this agreement with EmployeeScreenIQ. “Consumer Report” means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s character, general reputation, personal characteristics, mode of living, credit standing, or credit capacity, which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer’s eligibility for employment purposes. “Investigative Consumer Report” means a consumer report or portion thereof in which information on a consumer’s character, general reputation, personal characteristics, or mode of living is obtained through personal interviews with neighbors, friends, or associates of the consumer reported on or with others with whom he is acquainted or who may have knowledge concerning any such items of information. “Employment Purposes” means a report used for the purpose of evaluating a consumer for employment, promotion, reassignment or retention as an employee.

**2. GENERAL**

EmployeeScreenIQ strives to deliver accurate and timely information products to assist your company in making intelligent decisions for a permissible purpose under applicable law. To this end, EmployeeScreenIQ assembles information from a variety of sources, including information repositories, public records and third-party researchers. Please understand that these information sources and resources are not maintained by EmployeeScreenIQ. As a result, EmployeeScreenIQ cannot be a guarantor that the information provided from these sources is absolutely accurate or current. Nevertheless, EmployeeScreenIQ has in place procedures designed to respond promptly to claims of incorrect or inaccurate information in accordance with applicable laws. Likewise, User certifies that it also has in place reasonable procedures designed to comply with all applicable state and federal laws relating to background screening and equal employment opportunity.

**3. USER’S CERTIFICATION OF FCRA PERMISSIBLE PURPOSE(S)**

User hereby certifies that all orders for information products from EmployeeScreenIQ using User’s account shall be made, and the resulting reports shall be used, for the following Fair Credit Reporting Act (“FCRA”, at 15 U.S.C. § 1681 et seq.) permissible purposes only.

\_\_\_\_\_ **(Initial) Section 604(a)(3)(B). For employment purposes including evaluating a consumer for employment, promotion, reassignment or retention as an employee, where the consumer has given prior written permission.**

There are other permissible purposes for obtaining a consumer report. If your organization requires a consumer report for other permissible purposes, beyond employment, a new user agreement must be executed.

#### **4. USER'S CERTIFICATION OF LEGAL COMPLIANCE**

User hereby certifies to EmployeeScreenIQ that the information products it receives will not be used in violation of any applicable federal or state equal employment opportunity laws or regulations. User accepts full responsibility for using the information products it receives from EmployeeScreenIQ in a legally acceptable fashion and for the consequences of use and/or dissemination of those information products. As part of this commitment, User agrees to put into place reasonable policies and/or procedures to ensure the fair and equitable use of background information and to secure to the extent possible the confidentiality of each individual's private information. As one aspect of this commitment, User agrees to take precautionary measures to protect the security and dissemination of background information including but not limited to safeguarding access to such information by restricting access to terminal devices used to obtain such information, utilizing passwords to restrict access to such terminal devices, and securing access to, dissemination and destruction of hard copy reports. User further agrees to abide by the Access Security Requirements, attached hereto as Exhibit B. User certifies that it will retain any information it receives from EmployeeScreenIQ as well as applicant disclosure and authorization for a period of five years from the date the report was run as required in the Fair Credit Reporting Act.

#### **4.1 WHEN INFORMATION PRODUCTS ARE USED FOR EMPLOYMENT PURPOSES.**

If the information products are to be used for an employment purpose, User certifies that prior to obtaining or causing a "consumer report" and/or "investigative consumer report" to be obtained for employment purposes, a clear and conspicuous disclosure, in a document consisting solely of the disclosure, will be made in writing to the consumer explaining that a consumer report and/or investigative consumer report may be obtained for employment purposes, and will be presented to the consumer before the report is procured or caused to be procured. This disclosure will satisfy all requirements identified in Section 606(a)(1) of the Fair Credit Reporting Act as well as any applicable state or local laws. The consumer will have authorized, in writing, the obtaining of the report by User. User acknowledges that in order to complete some types of background screening searches, EmployeeScreenIQ will require the consumer's written authorization to be kept on file by EmployeeScreenIQ. EmployeeScreenIQ reserves the right to audit users process relating to consumer disclosure and authorization.

If the consumer is denied employment, or other adverse employment action taken in whole or in part on the basis of the report, User will provide to the consumer: (1) a copy of the report; and (2) a description, in writing, of the rights of the consumer entitled: "A Summary of Your Rights Under the Fair Credit Reporting Act." User hereby acknowledges that it has received a copy of the Summary of Rights (16 C.F.R. Part 601, Appendix A) and a Notice of User Responsibility (16 C.F.R. Part 601, Appendix C). These notices also are available at EmployeeScreenIQ's website (<http://www.employeescreen.com>), the Federal Trade Commission's website ([www.ftc.gov](http://www.ftc.gov)), and upon request by calling 1-800-235-3954.

#### **4.2 CONSUMER REPORTS**

If the consumer makes a written request within a reasonable amount of time, User will provide: (1) information about whether a consumer report has been requested; (2) if a consumer report has been requested, written disclosure of the nature and scope of the investigation requested; and (3) the name and address of the outside agency to whom requests for any of these reports has been made. This information will be provided no later than five days after the date on which the request for such disclosure was received from the consumer or such report was first requested, whichever is the latter.

#### **4.3 COMPLIANCE WITH STATE LAWS**

User certifies that it is aware that in addition to federal requirements in the FCRA, states may have their own distinct requirements. User agrees to keep itself informed of its obligations under both state and

federal laws and certifies that it will comply with all requirements under these laws, including the notice and authorization requirements. User further represents that any reports relating specifically to California residents or regarding transactions occurring in California will be ordered for the permissible purpose of pre-employment screening only.

## **5. ADDITIONAL REQUIREMENTS FOR DRIVING RECORDS**

User hereby certifies that Driving Records shall only be ordered in strict compliance with the Driver Privacy Protection Act (“DPPA”, at 18 U.S.C. § 2721 et seq.) and any related state laws. User further certifies that no Driving Record shall be ordered without first obtaining the written consent of the consumer, evidence of which shall be transmitted to EmployeeScreenIQ in the form of the consumer’s signed release authorization form. User also certifies that it will use this information only in the normal course of business to obtain lawful information relating to a holder of a commercial driver’s license or to verify information provided by an applicant or an employee. User shall not transmit any data contained in the resulting Driving Record via the public internet, electronic mail, or other unsecured means.

## **6. GENERAL PROVISIONS**

This agreement, including any exhibits, constitutes the entire agreement between the user and EmployeeScreenIQ. User agrees not to resell, sub-license, deliver, display or otherwise distribute to any third party any of the information products addressed herein, except as required by law. User may not assign or transfer this Agreement without the prior written consent of EmployeeScreenIQ. If any of the provisions of this Agreement become invalid, illegal or unenforceable in any respect under any law, the validity, legality and enforceability of the remaining provisions shall not in any way be effected or impaired. This Agreement shall be interpreted in accordance with the laws of the state of Ohio. All litigation arising out of this Agreement shall be commenced in Ohio, and the parties hereby consent to such jurisdiction and venue. Any written notice by either party shall be delivered personally by messenger, private mail courier service, or sent by registered or certified mail, return receipt requested, postage prepaid to the addresses listed below. This Agreement shall be construed as if it were jointly prepared. Both parties agree that this Agreement and all incorporations constitute all conditions of service, present and future. Changes to these conditions may be made only by mutual written consent of an authorized representative of a customer and an officer of EmployeeScreenIQ. The headings of each section shall have no effect upon the interpretation of any part of this Agreement.

## **7. FEES AND PAYMENT**

User agrees to pay fees and other charges which shall be nonrefundable for EmployeeScreenIQ background check services as set forth in the Subscriber Application. Such fee changes may be adjusted from time to time with prior written notice. Full payment must be made within thirty (30) days of the invoice date. At the option of EmployeeScreenIQ, payments not received thirty (30) days after the date of the invoice may cause the account to be placed on temporary interruption, with no additional requests being processed until the balance due is paid in full or arrangements have been made with our Accounts Payable Department. Accounts with invoices unpaid for thirty (30) days or more are subject to an interest charge of 1.5% per month, not to exceed the legal limit. User further agrees to pay any and all costs and expenditures related thereto, unless arrangements have been made with EmployeeScreenIQ Accounts Payable Department. If the account goes to collection, User agrees to pay all collection expenses, including attorneys’ fees and court costs. User hereby authorizes EmployeeScreenIQ to charge, without prior notice, any credit card of User for all or any portion of any payment due EmployeeScreenIQ from User.

## **8. WARRANTIES AND REMEDIES**

User understands that EmployeeScreenIQ obtains the information reported in its information products from various third party sources "AS IS", and therefore is providing the information to User "AS IS".

EmployeeScreenIQ makes no representation or warranty whatsoever, express or implied, including, but not limited to, implied warranties of merchantability or fitness for particular purpose, and implied warranties arising from the course of dealing or a course of performance with respect to the accuracy, validity, or completeness of any information products and/or consumer reports, that the information products will meet User's needs, or will be provided on an uninterrupted basis; EmployeeScreenIQ expressly disclaims any and all such representations and warranties. EmployeeScreenIQ will not be liable for any indirect, incidental, consequential, or special damages for loss of profits, whether incurred as a result of negligence or otherwise, even if EmployeeScreenIQ has been advised of the possibility of such damages. User understands that EmployeeScreenIQ' data is collected from and processed by sources which may be fallible, and that the compensation granted for said services is not a guarantee of accuracy. As such, User agrees to indemnify and hold harmless EmployeeScreenIQ, its successors and assigns, officers, directors, employees, agents and suppliers from any and all claims, actions or liabilities arising from or with respect to information products provided by EmployeeScreenIQ. User shall indemnify, defend and hold harmless EmployeeScreenIQ from and against any and all claims, suits, proceedings, damages, costs, expenses (including, without limitation, reasonable attorneys' fees and court costs) brought or suffered by any third party arising or resulting from, or otherwise in connection with, any breach by User of any of its representations, warranties, or agreements in this Agreement or its negligence or willful misconduct. In turn, EmployeeScreenIQ shall indemnify, defend and hold harmless User from and against any and all claims, suits, proceedings, damages, costs, expenses (including, without limitation, reasonable attorneys' fees and court costs) brought or suffered by any third party arising or resulting from, or otherwise in connection with, any breach by EmployeeScreenIQ of any of its representations, warranties, or agreements in this Agreement or its negligence or willful misconduct.

EmployeeScreenIQ cannot guarantee User's compliance with all applicable laws in its use of reported information, and makes no effort to provide compliance related services in connection with its furnishing of reports. User agrees that it will consult with its own legal or other counsel regarding the legality of using or relying on reported information in making employment decisions.

## **9. TERM AND TERMINATION**

This Section does not mandate exclusivity, minimum usage and/or guaranteed usage.

The term of this Agreement shall begin on the date it is executed by User and will continue for a period of one (1) year from that date, unless earlier terminated in writing. This Agreement will renew automatically for successive one (1) year periods unless either party gives written notice to the other party of its intent to terminate the Agreement. Such notice of intent to terminate must be given no less than thirty (30) days prior to the proposed termination date. EmployeeScreenIQ may terminate or revise the provisions of this Agreement immediately upon written notice if User is the debtor in a bankruptcy action or in an assignment for the benefit of creditors or in any other position of financial distress, or if User undergoes a change in ownership.

## **10. INTERNATIONAL USERS**

User understands that background information products from foreign countries and/or about foreign individuals are fraught with inherent limitations. The following is a non-exhaustive list of some reasons that such products may be inaccurate or incomplete: (1) The person indicated in the search may have committed a crime under a different name than that provided to EmployeeScreenIQ, there being no guarantee that courts will search for crimes committed under different names; (2) names may have variations in different countries; (3) the criminal

activity may be of a type not covered by EmployeeScreenIQ’s search capabilities; (4) the criminal activity may have been committed in a location not covered by EmployeeScreenIQ’s search capabilities; and/or (5) most countries do not maintain records in the same manner as the United States, inherently subjecting international searches to limitations. As a result of these and similar factors, EMPLOYEESCREENIQ HEREBY DISCLAIMS ANY WARRANTY OR IMPLICATION, IN ANY MANNER, THAT A SEARCH FOR INTERNATIONAL BACKGROUND INFORMATION WILL RESULT IN A COMPREHENSIVE AND/OR COMPLETE REPORT OF THE ACTIVITIES IN WHICH THE SUBJECT OF THE BACKGROUND CHECK MAY HAVE BEEN INVOLVED. This disclaimer is offered above and beyond those contained elsewhere in this Agreement given the inherent limitations associated with International background searches.

**11. FORCE MAJEURE**

User agrees that EmployeeScreenIQ is not responsible for any events or circumstances beyond its control (e.g., including but not limited to war, riots, embargoes, strikes and/or Acts of God) that prevent EmployeeScreenIQ from meeting its obligations under this Agreement.

**12. EXECUTION**

This Agreement may be executed in any number of counterparts, each of which shall be deemed an original, but all of which taken together shall constitute one and the same instrument. A signature on a copy of this Agreement received by either party by facsimile is binding upon the other party as an original. The parties shall treat a photocopy of such facsimile as a duplicate original. The individuals signing below represent that they are duly authorized to do so by and on behalf of the party for whom they are signing.

Authorized Signature	Date	EmployeeScreenIQ	Date
Printed Name		Printed Name	
Title		Title	
		EmployeeScreenIQ	
Company or Legal Business Name		4853 Galaxy Parkway, Bldg. K	
		Cleveland, Ohio 44128	
		Phone: (800) 235-3954	
		Fax: (888) 390-4617	

## EXHIBIT A –BILLING OPTIONS AND WEB USER INFORMATION

### BILLING OPTIONS

The EmployeeScreenIQ Bankers Online Affiliate Program requires screening services to be billed to a credit card. Your credit card will be charged at the end of the month for Consumer Reports completed within that month. You will still receive a monthly invoice but it will be marked as paid by credit card. For months in which there is no screening activity, there will be no charges invoiced or billed. Please write legibly.

Please charge my monthly invoice to my credit card:

#### Credit Card Charge Authorization

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

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

Card Holder: \_\_\_\_\_

Billing Address: \_\_\_\_\_

\_\_\_\_\_

Card Type:  Visa  Master Card  American Express

3 Digit Security Code: \_\_\_\_\_

Card Number: \_\_\_\_\_

Exp. Date: \_\_\_\_\_

I authorize EmployeeScreenIQ to charge my monthly invoice to the credit card listed above.

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



## EXHIBIT B – ACCESS SECURITY REQUIREMENTS

Business Name \_\_\_\_\_

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 employ an outside service provider to assist you. The credit reporting agency reserves the right to make changes to Access Security Requirements without notification. The information provided herewith provides minimum baselines for information security. In accessing the credit reporting agency's services, you agree to follow these security requirements:

### 1. IMPLEMENT STRONG ACCESS CONTROL MEASURES

- 1.1 Do not provide your credit reporting agency Subscriber Codes or passwords to anyone. No one from the credit reporting agency will ever contact you and request your Subscriber Code number or password.
- 1.2 Proprietary or third party system access software must have credit reporting agency Subscriber Codes and password(s) hidden or embedded. 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 of
- 1.4 Protect credit reporting agency Subscriber Code(s) and password(s) so that only key personnel know this sensitive information. Unauthorized personnel should not have knowledge of your Subscriber Code(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 credit reporting agency'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 credit reporting agency 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 (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 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 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 vigilantly 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** All credit reporting agency 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 credit reporting agency 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 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 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 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 credit reporting agency 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 25 months. In keeping with the ECOA, the credit reporting agency 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 breach or a consumer complaint that your company impermissibly accessed their credit report, the credit reporting agency 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.”

\_\_\_\_\_ (Initial) I have read and understand these requirements.