MacData Background Screening, LLC
609 S. Ridgewood Ave, Daytona Beach, FL 32114
386-254-4888 FAX 866-856-0367
www.macdata.com

MACDATA HAS ALL THE TOOLS YOU NEED FOR PRE-EMPLOYMENT BACKGROUND SCREENINGS!

We will need the following completed documents in order to activate your pre-employment background screening account:

- ☐ **Membership Application** form along with one of the listed documents to verify bona fide business entity.
- ☐ **Pre-Employment Screening Products and Pricing**. This form indicates which screening products you would like processed.
- ☐ **Payment and Invoicing Information** form.
- ☐ The **User Certification**. This form must be read and signed by each person accessing the consumer reports. Please feel free to make additional copies if necessary.
- ☐ The **Notice to Users of Consumer Reports** form. Please make copies for each User.
- ☐ The **Access Security Requirements** form. Please make copies for each User.
- ☐ Our **Non-Disclosure and Confidentiality Agreement**. Please make copies for each User.

Once your account has been activated, we will forward Online Instructions, User Name and Password along with the Employment Screening Release form. To obtain your applicant's consumer report, you must obtain either the signed Release form or order the report with **QuickApp™2.**

All applicants should receive a copy of the FCRA publication: **A Summary of Your Rights Under the Fair Credit Reporting Act,** available on our website: www.macdata.com.

If you have any questions, please do not hesitate to contact us.

We are proud members of the National Association of Professional Background Screeners.

MacData Background Screening, LLC
609 S. Ridgewood Ave, Daytona Beach, FL 32114
386-254-4888 FAX 866-856-0367
www.macdata.com

MEMBERSHIP APPLICATION

In order to comply with the Federal Trade Commission's Fair Consumer Reporting Act (FCRA), the following information and documentation must be completed in order to become a client of MacData Background Screening and begin receiving background screening reports. Once your online access is established, your User Name and Password will be provided along with personalized release forms for your screenings.

Important: All information must be completed in its entirety. Please print clearly and legibly to ensure accurate and timely processing.

Company Name: _____ Type of Business: _____

Mailing Address: _____ City_____ ST _____ Zip _____

Street Address: _____ City_____ ST _____ Zip _____

Phone: _____ Fax: _____

Principal or Authorized Agent of Company: _____ Title: _____

Email: _____ website: _____

Account Administrator: _____ Title: _____

Email: _____ Phone: _____

Is business located in? ☐ Commercial Building ☐ Private Residence

Permissible Purpose/Appropriate Use
In order to receive membership approval, you must substantiate that you are a legitimate business entity and have a legitimate permissible purpose for requesting consumer reports.

☐ Pre-Employment Background Screening – Please forward Bona Fide Business Entity documentation

☐ Tenant Background Screening – Please forward documentation from Page Two of our Membership Application

Proof of Bona Fide Business Entity – one Business Verification and one phone number verification document required

☐ **Please forward ONE of the following documents**

- Copy of Business License
- Business license status from a government web site (please include dated web print out)
- Experian approved Business Credit Report
- Articles of Incorporation with proof of filing

and

☐ **Telephone number verification – ONE of the following**

- Dated Screen Shot from Yellow Pages.com showing both the Directory Listing and Telephone number.
- A copy of Telephone Company billing statement showing both the Billing Party and Telephone number.

MacData Background Screening, LLC
609 S. Ridgewood Ave, Daytona Beach, FL 32114
386-254-4888 FAX 866-856-0367
www.macdata.com

PRE-EMPLOYMENT SCREENING PRODUCTS AND PRICING

All packages are customizable. If you have questions about a specific package, please contact our office for a price quote.

☐ **Basic Pre-Employment Package*.....$25.00**
- Identity Development - Name, Address, and SSN History
- InstaCriminal National /Sexual Offender**
- Choice of One Product from List A

☐ **Best Practices Pre-Employment Package.....$30.00**
- Same As Above plus County Criminal Records Search

* **County criminal record searches may be indicated dependent on results of InstaCriminal National Search.**
** **Alias and Maiden Name searches recommended.**
*** **County Criminal Record Search- Court Access Fees may apply.**

LIST A
(Choice of one product included in package price.)

☐ Global Homeland Security Search.....
☐ Bankruptcy Filings.....
☐ Lien and Judgment Filings.....

ADDITIONAL PRODUCTS

☐ InstaCriminal National/Sexual Offender Search - **Each Additional Name** $6.00
☐ County Criminal Record Search – Court Access Fees may apply $10.00
☐ Employment Verification $12.00
☐ Education Verification.....$12.00
☐ Professional Reference Verification $12.00
☐ Florida Driving Moving Violations – 7 Year $11.00
☐ Other States Driving Moving Violations.....Price varies per state
☐ CDLIS (Commercial Driving Records).....$5.00
☐ Experian Credit Report.....$15.00
☐ Bankruptcy Filings.....$5.00
☐ Lien and Judgment Filings.....$5.00
☐ Global Homeland Security Search.....$5.00
☐ Florida Department of Law Enforcement Criminal Record $36.00
☐ Credit Compliance Inspection to qualify to receive credit reports (One-time fee) $75.00
☐ Data Entry Fee for Emailed or Faxed Orders $5.00

DRUG SCREENING

☐ **5 Panel Drug Abuse Screening** $36.00
(Marijuana, Cocaine, Amphetamines, Opiates, Phencyclidine-PCP)

☐ **9 Panel Drug Abuse Screening** $39.00
(Marijuana, Cocaine, Amphetamines, Opiates, Phencyclidine-PCP, Methadone, Barbiturates, Benzodiazepines and Propoxyphene)

☐ **10 Panel Drug Abuse Screening** $40.00
(Marijuana, Cocaine, Amphetamines, Opiates, Phencyclidine-PCP, Methadone, Barbiturates, Benzodiazepines and Propoxyphene, Methaqualone)

☐ **Urine Alcohol Testing**.....$35.00

MacData Background Screening, LLC
609 S. Ridgewood Ave, Daytona Beach, FL 32114
386-254-4888 FAX 866-856-0367
www.macdata.com

PAYMENT AND INVOICING INFORMATION

Company Name: _____

Billing email address: _____
NOTE: Statements are sent out on a twice-monthly basis via email and USPS.

All screening requests must be paid upon ordering.

Please indicate your choice below and return this form along with your account set up packet.

☐ We would like to have a **credit card** kept on file.

_____
Cardholder's Name:

_____ _____ _____ _____
Cardholder's Billing Address: City: State: Zip:

Credit Card Type:
☐Master Card ☐VISA ☐American Express ☐Other _____

_____ _____ _____
Credit Card Number: Exp. Date: Verification Code:
(On signature line on back of card, this is the 3 or 4-digit # following last 4 digits of your credit card #)

I, the undersigned, authorize MacData Background Screening, LLC to bill requested screening services to this credit card.

X: _____ _____
Cardholder's Signature: Date:

☐ We would like to keep the above credit card on file, but would like the ability to enter an **alternate card** at the time of ordering.

☐ We will **enter the credit card information** each time we place an order.

FAX TO 1-866-856-0367 OR EMAIL TO: INFO@MACDATA.COM

MacData Background Screening, LLC
609 S. Ridgewood Ave, Daytona Beach, FL 32114
386-254-4888 FAX 866-856-0367
www.macdata.com

END USER CERTIFICATION FOR _____

(Business Name)

TO BE COMPLETED BY ACCOUNT ADMINSTRATOR:

1. Each authorized User must complete this form.
2. Alert our office when Users are no longer permitted access to your background screening account.
3. Please indicate the User Rights with your initials. Your signature is required for security purposes.

USER RIGHTS: Order Only _____; View Only _____; Order & View Only _____; Total Access _____

_____	_____	_____
Administrator Printed Name	Administrator Signature	Date

TO BE COMPLETED BY END USER:

End User acknowledges the following:

1. **The applicant has received and signed a written DISCLOSURE and AUTHORIZATION advising them that a consumer report, which may contain information as to their character, general reputation, personal characteristics and mode of living, whichever are applicable, will be processed. The business entity must retain the original document.**
2. **There is a permissible purpose for the background report.**
3. **The undersigned has read and understand their responsibilities under the *Notice to Users of Consumer Reports*.**
4. **The undersigned has read and understand their responsibilities for *Access Security*.**
5. **The undersigned has read and understand their responsibilities for *Non-Disclosure and Confidentiality*.**
6. **The undersigned certifies that they are the end user and will not further sell the information.**
7. **The undersigned understands that they will not use the information in the background report in violation of any federal or state equal opportunity laws.**
8. **The undersigned understands that they are responsible for providing the consumer with a copy of their report, along with the *Summary of Rights under the FCRA*.**
9. **The undersigned will follow adverse action procedures if a negative action is considered.**

Printed Name of End User: _____

Job Title: _____ Phone: _____

Email address: _____ Fax No. _____

End Users Month and Day of Birth (Used for Security) _____

SMS/Text-enabled cell phone number for MFA Security _____

Note: MFA allows User to authenticate with an email address; however, this is a less desirable method. For more information, see MFA Security Information page.

User Signature: _____ Date: _____

PLEASE FAX BACK TO: 866-856-0367 TOLL FREE OREMAIL TO: INFO@MACDATA.COM

MacData Background Screening, LLC
609 S. Ridgewood Ave, Daytona Beach, FL 32114
386-254-4888 FAX 866-856-0367
www.macdata.com

All users of consumer reports must comply with all applicable regulations, including regulations promulgated after this notice was first prescribed in 2004. Information about applicable regulations currently in effect can be found at the Consumer Financial Protection Bureau's website, www.consumerfinance.gov/learnmore.

NOTICE TO USERS OF CONSUMER REPORTS:
OBLIGATIONS OF USERS UNDER THE FCRA

The Fair Credit Reporting Act (FCRA),15 U.S.C. 1681-1681y, requires that this notice be provided to inform users of consumer reports of their legal obligations. State law may impose additional requirements. The text of the FCRA is set forth in full at the Bureau of Consumer Financial Protection's Website at www.consumerfinance.gov/learnmore. **Users must consult the relevant provisions of the FCRA for details about their obligations under the FCRA.**

The first section of this summary sets forth the responsibilities imposed by the FCRA on all users of consumer reports. The subsequent sections discuss the duties of users of reports that contain specific types of information, or that are used for certain purposes, and the legal consequences of violations. If you are a furnisher of information to a consumer reporting agency (CRA), you have additional obligations and will receive a separate notice from the CRA describing your duties as a furnisher.

I. OBLIGATIONS OF ALL USERS OF CONSUMER REPORTS

A. Users Must Have a Permissible Purpose

Congress has limited the use of consumer reports to protect consumers' privacy. All users must have a permissible purpose under the FCRA to obtain a consumer report. Section 604 contains a list of the permissible purposes under the law. These are:

- As ordered by a court or a federal grand jury subpoena. Section 604(a)(1)
- As instructed by the consumer in writing. Section 604(a)(2)
- For the extension of credit as a result of an application from a consumer, or the review or collection of a consumer's account. Section 604(a)(3)(A)
- For employment purposes, including hiring and promotion decisions, where the consumer has given written permission. Sections 604(a)(3)(B) and 604(b)2
- For the underwriting of insurance as a result of an application from a consumer. Section 604(a)(3)(C)
- When there is a legitimate business need, in connection with a business transaction that is initiated by the consumer. Section 604(a)(3)(F)(i)
- To review a consumer's account to determine whether the consumer continues to meet the terms of the account. Section 604(a)(3)(F)(ii)
- To determine a consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status. Section 604(a)(3)(D)
- For use by a potential investor or servicer, or current insurer, in a valuation or assessment of the credit or prepayment risks associated with an existing credit obligation. Section 604(a)(3)(E)
- For use by state and local officials in connection with the determination of child support payments, or modifications and enforcement thereof. Sections 604(a)(4) and 604(a)(5)

In addition, creditors and insurers may obtain certain consumer report information for the purpose of making "prescreened" unsolicited offers of credit or insurance. Section 604(c). The particular obligations of users of "prescreened" information are described in Section VII below.

B. Users Must Provide Certifications

Section 604(f) prohibits any person from obtaining a consumer report from a consumer reporting agency (CRA) unless the person has certified to the CRA the permissible purpose(s) for which the report is being obtained and certifies that the report will not be used for any other purpose.

C. Users Must Notify Consumers When Adverse Actions Are Taken

The term "adverse action" is defined very broadly by Section 603. "Adverse actions" include all business, credit, and employment actions affecting consumers that can be considered to have a negative impact as defined by Section 603(k) of the FCRA – such as denying or canceling credit or insurance, or denying employment or promotion. No adverse action occurs in a credit transaction where the creditor makes a counteroffer that is accepted by the consumer.

1. Adverse Actions Based on Information Obtained From a CRA

If a user takes any type of adverse action as defined by the FCRA that is based at least in part on information contained in a consumer report, Section 615(a) requires the user to notify the consumer. The notification may be done in writing, orally, or by electronic means. It must include the following:

- The name, address, and telephone number of the CRA (including a toll-free telephone number, if it is a nationwide CRA) that provided the report.
- A statement that the CRA did not make the adverse decision and is not able to explain why the decision was made.
- A statement setting forth the consumer's right to obtain a free disclosure of the consumer's file from the CRA if the consumer makes a request within 60 days.
- A statement setting forth the consumer's right to dispute directly with the CRA the accuracy or completeness of any information provided by the CRA.

2. Adverse Actions Based on Information Obtained From Third Parties Who Are Not Consumer Reporting Agencies
If a person denies (or increases the charge for) credit for personal, family, or household purposes based either wholly or partly upon information from a person other than a CRA, and the information is the type of consumer information covered by the FCRA, Section 615(b)(1) requires that the user clearly and accurately disclose to the consumer his or her right to be told the nature of the information that was relied upon if the consumer makes a written request within 60 days of notification. The user must provide the disclosure within a reasonable period of time following the consumer's written request.

3. Adverse Actions Based on Information Obtained From Affiliates
If a person takes an adverse action involving insurance, employment, or a credit transaction initiated by the consumer, based on information of the type covered by the FCRA, and this information was obtained from an entity affiliated with the user of the information by common ownership or control, Section 615(b)(2) requires the user to notify the consumer of the adverse action. The notice must inform the consumer that he or she may obtain a disclosure of the nature of the information relied upon by making a written request within 60 days of receiving the adverse action notice. If the consumer makes such a request, the user must disclose the nature of the information not later than 30 days after receiving the request. If consumer report information is shared among affiliates and then used for an adverse action, the user must make an adverse action disclosure as set forth in I.C.1 above.

D. Users Have Obligations When Fraud and Active Duty Military Alerts are in Files
When a consumer has placed a fraud alert, including one relating to identity theft, or an active duty military alert with a nationwide consumer reporting agency as defined in Section 603(p) and resellers, Section 605A(h) imposes limitations on users of reports obtained from the consumer reporting agency in certain circumstances, including the establishment of a new credit plan and the issuance of additional credit cards. For initial fraud alerts and active duty alerts, the user must have reasonable policies and procedures in place to form a belief that the user knows the identity of the applicant or contact the consumer at a telephone number specified by the consumer; in the case of extended fraud alerts, the user must contact the consumer in accordance with the contact information provided in the consumer's alert.

E. Users Have Obligations When Notified of an Address Discrepancy
Section 605(h) requires nationwide CRAs, as defined in Section 603(p), to notify users that request reports when the address for a consumer provided by the user in requesting the report is substantially different from the addresses in the consumer's file. When this occurs, users must comply with regulations specifying the procedures to be followed, which will be issued by the Federal Trade Commission and the banking and credit union regulators. The Consumer Financial Protection Bureau regulations will be available at www.consumerfinance.gov/learnmore.

F. Users Have Obligations When Disposing of Records
Section 628 requires that all users of consumer report information have in place procedures to properly dispose of records containing this information. The Federal Trade Commission, the Securities and Exchange Commission, and the banking and credit union regulators have issued regulations covering disposal. The Consumer Financial Protection Bureau regulations may be found at www.consumerfinance.gov/learnmore.

II. CREDITORS MUST MAKE ADDITIONAL DISCLOSURES

If a person uses a consumer report in connection with an application for, or a grant, extension, or provision of, credit to a consumer on material terms that are materially less favorable than the most favorable terms available to a substantial proportion of consumers from
or through that person, based in whole or in part on a consumer report, the person must provide a risk-based pricing notice to the consumer in accordance with regulation prescribed by the Consumer Financial Protection Bureau.
Section 609(g) requires a disclosure by all persons that make or arrange loans secured by residential real property (one to four units) and that use credit scores. These persons must provide credit scores and other information about credit scores to applicants, including the disclosure set forth in Section 609(g)(1)(D) ("Notice to the Home Loan Applicant").

III. OBLIGATIONS OF USERS WHEN CONSUMER REPORTS ARE OBTAINED FOR EMPLOYMENT PURPOSES

A. Employment Other Than in the Trucking Industry
If information from a CRA is used for employment purposes, the user has specific duties, which are set forth in Section 604(b) of the FCRA. The user must:

- Make a clear and conspicuous written disclosure to the consumer before the report is obtained, in a document that consists solely of the disclosure, that a consumer report may be obtained.
- Obtain from the consumer prior written authorization. Authorization to access reports during the term of employment may be obtained at the time of employment.
- Certify to the CRA that the above steps have been followed, that the information being obtained will not be used in violation of any federal or state equal opportunity law or regulation, and that, if any adverse action is to be taken based on the consumer report, a copy of the report and a summary of the consumer's rights will be provided to the consumer.
- **Before** taking an adverse action, the user must provide a copy of the report to the consumer as well as the summary of consumer's rights. (The user should receive this summary from the CRA.) A Section 615(a) adverse action notice should be sent after the adverse action is taken.

An adverse action notice also is required in employment situations if credit information (other than transactions and experience data) obtained from an affiliate is used to deny employment. Section 615(b)(2) The procedures for investigative consumer reports and employee misconduct investigations are set forth below.

B. Employment in the Trucking Industry
Special rules apply for truck drivers where the only interaction between the consumer and the potential employer is by mail, telephone, or computer. In this case, the consumer may provide consent orally or electronically, and an adverse action may be made orally, in writing, or electronically. The consumer may obtain a copy of any report relied upon by the trucking company by contacting the company.

IV. OBLIGATIONS WHEN INVESTIGATIVE CONSUMER REPORTS ARE USED

Investigative consumer reports are a special type of consumer report in which information about a consumer's character, general reputation, personal characteristics, and mode of living is obtained through personal interviews by an entity or person that is a consumer reporting agency. Consumers who are the subjects of such reports are given special rights under the FCRA. If a user intends to obtain an investigative consumer report, Section 606 requires the following:

- The user must disclose to the consumer that an investigative consumer report may be obtained. This must be done in a written disclosure that is mailed, or otherwise delivered, to the consumer at some time before or not later than three days after the date on which the report was first requested. The disclosure must include a statement informing the consumer of his or her right to request additional disclosures of the nature and scope of the investigation as described below, and the summary of consumer rights required by Section 609 of the FCRA. (The summary of consumer rights will be provided by the CRA that conducts the investigation.)
- The user must certify to the CRA that the disclosures set forth above have been made and that the user will make the disclosure described below.
- Upon the written request of a consumer made within a reasonable period of time after the disclosures required above, the user must make a complete disclosure of the nature and scope of the investigation. This must be made in a written statement that is mailed, or otherwise delivered, to the consumer no later than five days after the date on which the request was received from the consumer or the report was first requested, whichever is later in time.

V. SPECIAL PROCEDURES FOR EMPLOYEE INVESTIGATIONS

Section 603(x) provides special procedures for investigations of suspected misconduct by an employee or for compliance with Federal, state or local laws and regulations or the rules of a self-regulatory organization, and compliance with written policies of the employer. These investigations are not treated as consumer reports so long as the employer or its agent complies with the procedures set forth in Section 603(x), and a summary describing the nature and scope of the inquiry is made to the employee if an adverse action is taken based on the investigation.

VI. OBLIGATIONS OF USERS OF MEDICAL INFORMATION

Section 604(g) limits the use of medical information obtained from consumer reporting agencies (other than payment information that appears in a coded form that does not identify the medical provider). If the information is to be used for an insurance transaction, the consumer must give consent to the user of the report or the information must be coded. If the report is to be used for employment purposes – or in connection with a credit transaction (except as provided in regulations issued by the banking and credit union regulators) – the consumer must provide specific written consent and the medical information must be relevant. Any user who receives medical information shall not disclose the information to any other person (except where necessary to carry out the purpose for which the information was disclosed, or as permitted by statute, regulation, or order).

VII. OBLIGATIONS OF USERS OF "PRESCREENED" LISTS

The FCRA permits creditors and insurers to obtain limited consumer report information for use in connection with unsolicited offers of credit or insurance under certain circumstances. Sections 603(l), 604(c), 604(e), and 615(d). This practice is known as "prescreening" and typically involves obtaining from a CRA a list of consumers who meet certain preestablished criteria. If any person intends to use prescreened lists, that person must (1) before the offer is made, establish the criteria that will be relied upon to make the offer and to grant credit or insurance, and (2) maintain such criteria on file for a three-year period beginning on the date on which the offer is made to each consumer. In addition, any user must provide with each written solicitation a clear and conspicuous statement that:

- Information contained in a consumer's CRA file was used in connection with the transaction.
- The consumer received the offer because he or she satisfied the criteria for credit worthiness or insurability used to screen for the offer.
- Credit or insurance may not be extended if, after the consumer responds, it is determined that the consumer does not meet the criteria used for screening or any applicable criteria bearing on credit worthiness or insurability, or the consumer does not furnish required collateral.
- The consumer may prohibit the use of information in his or her file in connection with future prescreened offers of credit or insurance by contacting the notification system established by the CRA that provided the report. The statement must include the address and toll-free telephone number of the appropriate notification system.

In addition, the Consumer Financial Protection Bureau has established the format, type size, and manner of the disclosure required by Section 615(d), with which users must comply. The relevant regulation is 12 CFR 1022.54.

VIII. OBLIGATIONS OF RESELLERS

A. Disclosure and Certification Requirements

Section 607(e) requires any person who obtains a consumer report for resale to take the following steps:

- Disclose the identity of the end-user to the source CRA.
- Identify to the source CRA each permissible purpose for which the report will be furnished to the end-user.
- Establish and follow reasonable procedures to ensure that reports are resold only for permissible purposes, including procedures to obtain:
  1. the identity of all end-users;
  2. certifications from all users of each purpose for which reports will be used; and
  3. certifications that reports will not be used for any purpose other than the purpose(s) specified to the reseller. Resellers must make reasonable efforts to verify this information before selling the report.

B. Reinvestigations by Resellers

Under Section 611(f), if a consumer disputes the accuracy or completeness of information in a report prepared by a reseller, the reseller must determine whether this is a result of an action or omission on its part and, if so, correct or delete the information. If not, the reseller must send the dispute to the source CRA for reinvestigation. When any CRA notifies the reseller of the results of an investigation, the reseller must immediately convey the information to the consumer.

C. Fraud Alerts and Resellers

Section 605A(f) requires resellers who receive fraud alerts or active duty alerts from another consumer reporting agency to include these in their reports.

IX. LIABILITY FOR VIOLATIONS OF THE FCRA

Failure to comply with the FCRA can result in state government or federal government enforcement actions, as well as private lawsuits. Sections 616, 617, and 621. In addition, any person who knowingly and willfully obtains a consumer report under false pretenses may face criminal prosecution. Section 619.

MacData Background Screening, LLC
609 S. Ridgewood Ave, Daytona Beach, FL 32114
386-254-4888 FAX 866-856-0367
www.macdata.com

Access Security Requirements

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. Capitalized terms used herein have the meaning given in the Glossary attached hereto. 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 passwords to anyone. No one from the credit reporting agency will ever contact you and request your password.

1.2 Proprietary or third party system access software must have password(s) hidden or embedded. Account numbers and passwords should be known only by supervisory personnel.

1.3 You must request your password be changed immediately when:
- any system access software is replaced or is no longer used;
- the hardware on which the software resides is upgraded, changed or disposed of

1.4 Protect password(s) so that only key personnel know this sensitive information. Unauthorized personnel should not have knowledge of your 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 entireinformation 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 standalone computers that directly access the Internet must have a desktop Firewall deployed that is installed and configured to block unnecessary/unused ports, services and network traffic.

5.5 Encrypt Wireless access points with a minimum of WEP 128 bit encryption, WPA encryption where available.

5.6 Disable vendor default passwords, SSIDs and IP Addresses on Wireless access points and restrict authentication on the configuration of the access 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."

MacData Background Screening, LLC
609 S. Ridgewood Ave, Daytona Beach, FL 32114
386-254-4888 FAX 866-856-0367
www.macdata.com

NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT

In connection with a possible business transaction (the 'Transaction') involving the parties hereto, either party may disclose certain information to the other party which is non-public confidential information (the "Disclosing Party" and "Receiving Party," respectively). All information (including, without limitation, software, designs, drawings, specifications, techniques, models, data, source code, object code, documentation, diagrams, flow charts, research, development, processes, procedures, marketing plans, customer information, price lists, pricing policies and financial information) disclosed (whether in writing, electronically or orally) be the Disclosing Party or its directors, officers, employees, affiliates or representatives of advisors, including counsel, lenders and financial advisors (collectively, the "Representatives") to the Receiving Party or its Representatives and all analyses, compilations, forecasts and other studies or other documents prepared by the Disclosing Party or the Receiving Party, or their respective Representatives, in connection with the Receiving Party's review of the Transaction which contain or reflect such information is hereinafter referred to as the "Information." The term "Information" will not, however, include information which (i) at the time of disclosure or thereafter is generally available to and known by the public (other than as a result of a disclosure directly or indirectly be either party or their respective Representatives in violation of this Agreement), (ii) at the time of disclosure was available on the non-confidential basis from a source other than the Disclosing Party or its Representatives, provided that such source is not and was not bound by a confidentiality agreement with the Disclosing Party, or (iii) was known by the Receiving Party prior to receiving the information from the Disclosing Party or has been independently acquired or developed by the Receiving Party without violating any of its obligations under this Agreement.

Accordingly, both parties hereby agree that:

1. The parties recognize and agree that the information is the property of the Disclosing Party and will be furnished to the receiving Party in reliance upon the undertakings of the Receiving Party made herein. The Receiving Party and its Representatives (i) will keep the information confidential and will not (except as required by applicable law and only after compliance with paragraph 3 below), disclose any information, and (ii) will not use any information in any way detrimental to the Disclosing Party of its shareholders or for any purpose other than in connection with the Transaction; provided, however, that the Receiving Party may reveal the Information to its Representatives (a) who need to know the Information for the purpose of evaluating the Transaction, (b) who are informed by the Receiving Party of the confidential nature of the Information, and (c) who agree to be bound by the terms of this Agreement. Each party will cause its Representatives to observe the terms of this Agreement, and the respective party will be responsible for any breach of this Agreement by any of its Representatives.

2. Without prior written consent, neither party nor its Representatives will (except as required by applicable law, regulation or legal process, and only after compliance with paragraph 3 below) disclose to any person the fact that the Information exists or has been made available, that they are considering the Transaction or that discussions or negotiations between the parties are taking or have taken place concerning the Transaction. The term "person" as used in this Agreement will be interpreted broadly to include, without limitation, any corporation, company, limited liability company, partnership, or individual.

3. In the event that the Receiving Party or any of its Representatives are required by applicable law to disclose any of this information, they will notify the Disclosing Party promptly in writing of such requirement so that it may seek a protective order or other appropriate remedy, or, in its sole discretion, waive compliance with the terms of this Agreement and deliver such waiver in writing to the Receiving Party. In the event that no such protective order or other remedy is obtained, or that the Disclosing Party waives compliance with the terms of this Agreement, the Receiving Party will furnish only that portion of the Information which it is advised by counsel is legally required and will exercise its best efforts to obtain reliable assurance that confidential treatment will be accorded the Information. Notwithstanding anything in the Agreement to the contrary, the Receiving Party may upon notice to the other party disclose the Information in connection with the proposed Transaction or otherwise, if, in the written opinion of that party's legal counsel, such disclosure is required by the federal securities laws.

4. The Receiving Party agrees and acknowledges that the Information is and shall remain the sole and exclusive property of the Disclosing Party and that no license or similar proprietary right is granted to the Receiving Party hereunder.

5. If either party determines not to proceed with the Transaction, it will promptly inform the other party of that decision in writing and, in that case, and at any time upon the request of the Disclosing Party, the Receiving Party will either (i) promptly destroy all originals, copies, extracts, or other reproductions in whole or in part of such written material Information, in its or its Representatives' possession then notify the Disclosing Party in writing that such written material Information has been destroyed, or (ii) promptly deliver to the Disclosing Party at the Receiving Party's own expense all originals, copies, extracts, or other reproduction in whole or in part of such written material Information on its or its Representatives' possession. Any oral Information will continue to be subject to the terms of this Agreement.

6. Both parties acknowledge that neither party, nor its Representative, nor any of their respective officers, directors, employees, agents or controlling persons, makes any express or implied representation or warranty as to the accuracy or completeness of the Information. Each party further agrees that it is not entitled to rely on the accuracy or completeness of the Information and that it will be entitled to rely solely on such representations and

warranties as may be included in any definitive agreement with respect to the Transaction, subject to such limitations and restrictions as may be contained therein. The parties acknowledge and agree that unless and until a written definitive agreement concerning the Transaction has been executed; neither party has any oblation to enter into the Transaction or any other transaction.

7. Both parties are aware and will advise their representatives, who are informed of the matters that are the subject of this Agreement, of the restrictions imposed by the United States securities laws on the purchase or sale of securities by any person who has received material, non-public information from the issuer of such securities and on the communication of such information to any person when it is reasonable foreseeable that such other person is likely to purchase or sell such securities if reliance upon such information.

8. Both parties acknowledge that remedies at law may be inadequate to protect the Disclosing Party against any actual or threatened breach of this Agreement by the Receiving Party or by its Representatives, and, without prejudice to any other rights and remedies otherwise available to the Disclosing Party, the Receiving Party agrees to the granting of competent jurisdiction determines in a final, non-appealable order that the Agreement has been breached by either party or by its Representatives, then the Receiving Party will reimburse the Disclosing Party for its costs and expenses (including, without limitation, legal fees and expenses) incurred in connection with all such litigation.

9. This Agreement will be governed by and construed in accordance with the laws of Florida, without giving effect to its conflict of laws, principles or rules. Each party hereby irrevocable and unconditionally agrees that any actions, suits or proceedings arising out of or relating to this Agreement will be submitted to binding arbitration in Volusia County, Florida, before a retiring judge associated with Judicial Arbitration and Mediation Service, Inc., as the exclusive remedy for such claim or dispute.

10. It is understood and agreed that both parties are entitled to enforce the terms of this Agreement and that all rights hereunder shall inure to the benefit of the parties and their assigns. The parties agree that no failure or delay in a party's exercising any right, power or privilege hereunder will operate as a waiver thereof, nor will any single or partial exercise thereof preclude any other or further exercise thereof or the exercise of any right, power or privilege hereunder.

11. Each party agrees that for a period of two years after the later of the date hereof or the consummation of the Transaction, such party shall not disrupt, damage, impair or interfere with each other's business in any manner, including, without limitation, by directly or indirectly soliciting or inducing or attempting to solicit or induce any employee of the other party to leave the employ of that party, or by inducing an employee, a consultant, or an independent contractor to sever or modify that person's relationship with that party, by interfering with or raiding each other's employees, disrupting their relationships with customers, agents, representatives or vendors, or otherwise.

12. This Agreement contains the entire agreement between the parties concerning the subject matter hereof, and no modifications of this Agreement or waiver of the terms and conditions hereof will be binding upon a party, unless approved in writing by such party. If any of the provision set forth in this Agreement are not enforceable, in whole or in part. The remaining provisions set forth in this Agreement shall nonetheless remain enforceable. Any provision not enforceable in part shall be enforced to the extent valid and enforceable. It is further understood and agreed that no failure or delay by either party in exercising any right, power or privilege hereunder will operate as a waiver thereof, nor will any single or partial exercise thereof preclude any other or further exercise thereof or the exercise of any right, power or privilege hereunder. Neither party may assign its obligations under this Agreement.