Burgess Smith

From: agorzelsky@creditrelatedinfo.com
Sent: Monday, April 10, 2017 4:07 PM
To: burgess@raystownrealty.com
Subject: Information for Tenant Screening
Attachments: Access Security Requirements.pdf; Credit Scoring Agreement.doc; EU FCRA Requirements[1].doc; Membership Application for Landlords.doc

Follow Up Flag: Follow up
Flag Status: Flagged

Attached is the paperwork that would need completed in order for you to be able to get credit reports. In addition to that I will also need the following:

1. Copy of your photo ID
2. List of the addresses of your rental properties (this can be in the form of an email or on letterhead)
3. Tax assessments or deeds for each of your rental properties
4. 3 completed and signed rental applications from perspective tenants only have one pending.

Once you have returned all the paperwork to me, I can then schedule your inspection. If you work out of your residence, the inspection is required annually and the fee is $110. If you have a commercial office, it is one time inspection and the cost is the same, $110. Please let me know if you have any questions. Thank you and have a great day!

Angela M. Gorzelsky

Manager

Johnstown Credit Bureau, Inc.

Ph: (814) 535-2513

Fax: (814) 535-3364

www.creditrelatedinfo.com

Property Address.

① 308 2nd Street
Hemlingdon Pa 16652
owned by Anthony & Associates LLC
I am owner.

② 3040 Coco Spring Rd
Hemlingdon PA 16652
owned by myself & wife mary Jane Smith

"Your Regional Provider of Credit Related Information Products

RAYSTOWN REALTY, INC.
BURGESS A. SMITH
310 2ND STREET
HUNTINGDON, PA 16652

KISH BANK
BELLEVILLE, PA 17004
60-1055/313

2734

4/11/2017

PAY TO THE ORDER OF Johnstown Credit Bureau, Inc $ **110.00

One Hundred Ten and 00/100********** DOLLARS

Johnstown Credit Bureau, Inc
2355 Bedford Street, Suite 4
Johnstown, Pa 15904

MEMO tenant credit check

AUTHORIZED SIGNATURE

⑈002734⑈ ⑆031310552⑆ 12⑈854⑈6⑈

Huntingdon County Online Information System

Parcel Number 17-03-158

Parcel Information

District	HUNTINGDON BORO - 17
Parcel Number	17-03-158
Property Address	308 2ND STREET
Acres	0.07
Property Type	RESIDENTIAL
School District	HUNTINGDON AREA

Current Deed Book/Page	705/785
Property ID	8292
Date of Sale	3/15/2004
Selling Price	$1
Tax Claim	CALL (814) 643-3526 FOR STATUS

Name and Street Address

Business Smith President

Owner List	ANTHONY AND ASSOCIATES LLC
Owner Address	ANTHONY AND ASSOCIATES LLC 310 SECOND ST HUNTINGDON, PA 16652
Description	RESIDENTIAL

2017 Taxes

Taxes are Estimates Only

County	$176.80
Cty Special 911	$0.00
Cty Special Bailey	$0.00
Township	$195.84
School	$439.01
Total	**$811.65**

Property Values

Assessment Information	
Land	$1,440
Improvements	$9,440
Total Assessment	**$10,880**

Clean and Green	
Approved?	NO
Land	
Improvements	
Total Assessment	

Additional Information	
Homestead	NO
Farm Outbuildings	

Building Market Assessment

Buildings Market Values	
Residential	$11,800
Outbuildings	
Total	**$11,800**

Outbuildings Market Values				
Type	**Year**	**Length**	**Width**	**Value**

Description

Dwelling Type	BUILDING - PRIVATE	**Bedrooms**	
Stories		**Full Baths**	
Actual Age	OLD	**Half Baths**	
Remodeled Date		**Heating**	
Basement		**Air Conditioning**	
Basement Garage		**Public Water**	Y
Exterior		**Public Sewer**	Y
First Level Rooms		**Fireplaces**	
Second Level Rooms		**Pool**	
Third Level Rooms		**Paved Streets**	A

Department of Treasury
Internal Revenue Service
Philadelphia Service Center

FAX MESSAGE

Date: 5/12/98

To: BURGESS A SMITH

Phone Number:
Fax Phone Number: 8814-643-4774

From: Tele-Tin, Michelle Trinacria
Address: 11601 Roosevelt Blvd, DP 334
Philadelphia, PA 19154
Phone: 215-516-6999
Fax Phone: 215-516-3990

Subject: Per Your Request, Your employer identification number is: 25-1810053/ ANTHONY AND ASSOCIATES, LLC

CONFIDENTIAL NOTICE

Huntingdon County Online Information System

Parcel Number 34-07-36.1

Parcel Information

District	ONEIDA TWP - 34
Parcel Number	34-07-36.1
Property Address	3640 COLD SPRINGS ROAD
Acres	0.48
Property Type	RESIDENTIAL
School District	HUNTINGDON AREA

Current Deed Book/Page	544/244
Property ID	15978
Date of Sale	8/11/2000
Selling Price	$70,000
Tax Claim	CALL (814) 643-3526 FOR STATUS

Name and Street Address

Owner List	SMITH BURGESS A & MARY JANE E
Owner Address	SMITH BURGESS A & MARY JANE E 310 2ND ST HUNTINGDON PA 16652
Description	RESIDENTIAL

2017 Taxes

Taxes are Estimates Only

County	$357.50
Cty Special 911	$0.00
Cty Special Bailey	$0.00
Township	$44.00
School	$887.70
Total	**$1,289.20**

Property Values

Assessment Information	
Land	$2,720
Improvements	$19,280
Total Assessment	**$22,000**

Clean and Green	
Approved?	NO
Land	
Improvements	
Total Assessment	

Additional Information	
Homestead	NO
Farm Outbuildings	

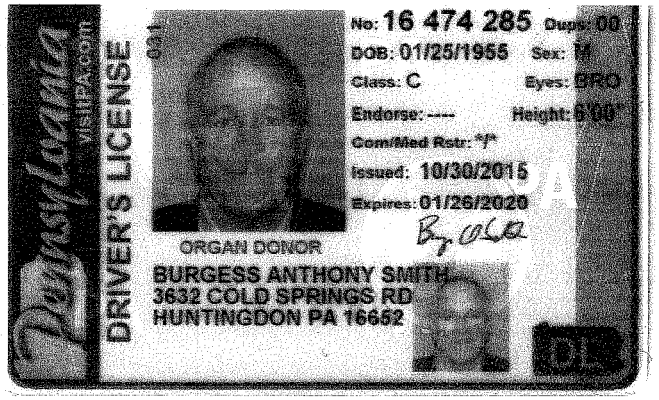
Building Market Assessment

Buildings Market Values	
Residential	$24,100
Outbuildings	
Total	**$24,100**

Outbuildings Market Values				
Type	**Year**	**Length**	**Width**	**Value**

Description

Dwelling Type	BUILDING - PRIVATE	**Bedrooms**	03
Stories		**Full Baths**	
Actual Age	1979	**Half Baths**	
Remodeled Date		**Heating**	ELECTRIC
Basement	FULL	**Air Conditioning**	
Basement Garage		**Public Water**	N
Exterior	ALUMINUM, BRICK	**Public Sewer**	N
First Level Rooms	05	**Fireplaces**	
Second Level Rooms		**Pool**	
Third Level Rooms		**Paved Streets**	A


Pennsylvania
VISITPA.com
DRIVER'S LICENSE
SAMPLE
ORGAN DONOR
BURGESS ANTHONY SMITH
3632 COLD SPRINGS RD
HUNTINGDON PA 16652
No: 16 474 285 Dupe: 00
DOB: 01/25/1955 Sex: M
Class: C Eyes: BRO
Endorse: ---- Height: 6'00"
Com/Med Restr: "I"
Issued: 10/30/2015
Expires: 01/26/2020

Johnstown Credit Bureau, Inc.
2355 Bedford Street, Suite 4
Johnstown, PA 15904
PH: (814) 535-2513
FAX: (814) 535-3364

Access Security Requirements for FCRA and GLB 5A Data

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

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

1. **Implement Strong Access Control Measures**

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

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

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

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

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

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

1.7 Develop strong passwords that are:

- Not easily guessable (i.e. your name or company name, repeating numbers and letters or consecutive numbers and letters)
- Contain a minimum of eight (8) alphabetic and numeric characters for standard user accounts
- For interactive sessions (i.e. non system-to-system) ensure that passwords/passwords are changed periodically (every 90 days is recommended)

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

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

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

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

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

1.12 Ensure that personnel who are authorized access to credit information have a business need to access such information and understand these requirements to access such information are only for the permissible purposes listed in the Permissible Purpose Information section of the membership application.

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

1.14 Ensure that Company employees do not access their own credit reports or those reports of any family member(s) or friend(s) unless it is in connection with a credit transaction or for another permissible purpose.

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

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

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

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

2. Maintain a Vulnerability Management Program

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

2.2 Configure infrastructure such as firewalls, routers, servers, tablets, smart phones, personal computers (laptops and desktops), and similar components to industry best security practices, including disabling unnecessary services or features, and removing or changing default passwords, IDs and sample files/programs, and enabling the most secure configuration features to avoid unnecessary risks.

2.3 Implement and follow current best security practices for computer virus detection scanning services and procedures:

- Use, implement and maintain a current, commercially available anti-virus software on all systems, if applicable anti-virus technology exists. Anti-virus software deployed must be capable to detect, remove, and protect against all known types malicious software such as viruses, worms, spyware, adware, Trojans, and root-kits.
- Ensure that all anti-virus software is current, actively running, and generating audit logs; ensure that anti-virus software is enabled for automatic updates and performs scans on a regular basis.
- If you suspect an actual or potential virus infecting a system, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.

3. Protect Data

3.1 Develop and follow procedures to ensure that data is protected throughout its entire information lifecycle (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.).

3.2 Experian data is classified Confidential and must be secured to in accordance with the requirements mentioned in this document at a minimum.

3.3 Procedures for transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.

3.4 Encrypt all Experian data and information when stored electronically on any system including but not limited to laptops, tablets, personal computers, servers, databases using strong encryption such AES 256 or above.

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

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

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

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

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

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

4. Maintain an Information Security Policy

4.1 Develop and follow a security plan to protect the confidentiality and integrity of personal consumer information as required under the GLB Safeguards Rule.

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

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

4.4 The FACTA Disposal Rules requires that Company implement appropriate measures to dispose of any sensitive information related to consumer credit reports and records that will protect against unauthorized access or use of that information.

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

4.6 When using third party service providers (e.g. application service providers) to access, transmit, store or process Experian data, ensure that service provider is compliant with Experian Independent Third Party Assessment (EI3PA) program, and registered in Experian list of compliant service providers. If the service provider is in process of becoming compliant, it is Company responsibility to ensure the service provider is engaged with Experian and exception is granted in writing. *Approved certifications in lieu of EI3PA can be found in the Glossary section.*

5. Build and Maintain a Secure Network

5.1 Protect Internet connections with dedicated, industry-recognized firewalls that are configured and managed using industry best security practices.

5.2 Internal private Internet Protocol (IP) addresses must not be publicly accessible or natively routed to the Internet. Network address translation (NAT) technology should be used.

5.3 Administrative access to firewalls and servers must be performed through a secure internal wired connection only.

5.4 Any stand-alone computers that directly access the Internet must have a desktop firewall deployed that is installed and configured to block unnecessary/unused ports, services, and network traffic.

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

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

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

6. Regularly Monitor and Test Networks

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

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

6.3 Use current best practices to protect telecommunications systems and any computer system or network device(s) used to provide Services hereunder to access Experian systems and networks. These controls should be selected and implemented to reduce the risk of infiltration, hacking, access penetration or exposure to an unauthorized third party by:

- protecting against intrusions;
- securing the computer systems and network devices;
- and protecting against intrusions of operating systems or software.

7. Mobile and Cloud Technology

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

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

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

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

7.5 Mobile applications and data shall be hosted on devices through a secure container separate from any personal applications and data. See details below. Under no circumstances is Experian data to be exchanged between secured and non-secured applications on the mobile device.

7.6 In case of non-consumer access, that is, commercial/business-to-business (B2B) users accessing Experian data via mobile applications (internally developed or using a third party application), ensure that multi-factor authentication and/or adaptive/risk-based authentication mechanisms are utilized to authenticate users to application.

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

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

8. General

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

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

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

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

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

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

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

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

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

8.7 Company shall report actual security violations or incidents that impact Experian to Experian within twenty-four (24) hours or per agreed contractual notification timeline. Company agrees to provide notice to Experian of any confirmed security breach that may involve data related to the contractual

relationship, to the extent required under and in compliance with applicable law. Telephone notification is preferred at 800-295-4305, Email notification will be sent to regulatorycompliance@experian.com .

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

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

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

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

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

"Under Section 621 (a) (2) (A) of the FCRA, any person that violates any of the provisions of the FCRA may be liable for a civil penalty of not more than $3,500 per violation."

Internet Delivery Security Requirements

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

General requirements:

1. The Company shall designate in writing, an employee to be its Head Security Designate, to act as the primary interface with Experian on systems access related matters. The Company's Head Security Designate will be responsible for establishing, administering and monitoring all Company employees' access to Experian provided services which are delivered over the Internet ("Internet access"), or approving and establishing Security Designates to perform such functions.
2. The Company's Head Security Designate or Security Designate shall in turn review all employee requests for Internet access approval. The Head Security Designate or its Security Designate shall determine the appropriate access to each Experian product based upon the legitimate business needs of each employee. Experian shall reserve the right to terminate any accounts it deems a security threat to its systems and/or consumer data.
3. Unless automated means become available, the Company shall request employee's (Internet) user access via the Head Security Designate/Security Designate in writing, in the format approved by Experian. Those employees approved by the Head Security Designate or Security Designate for Internet access ("Authorized Users") will be

individually assigned unique access identification accounts ("User ID") and passwords/passphrases (this also applies to the unique Server-to-Server access IDs and passwords/passphrases). Experian's approval of requests for (Internet) access may be granted or withheld in its sole discretion. Experian may add to or change its requirements for granting (Internet) access to the services at any time (including, without limitation, the imposition of fees relating to (Internet) access upon reasonable notice to Company), and reserves the right to change passwords/passphrases and to revoke any authorizations previously granted. *Note: Partially completed forms and verbal requests will not be accepted.*

4. An officer of the Company agrees to notify Experian in writing immediately if it wishes to change or delete any employee as a Head Security Designate, Security Designate, or Authorized User; or if the identified Head Security Designate, Security Designate or Authorized User is terminated or otherwise loses his or her status as an Authorized User.

Roles and Responsibilities

1. Company agrees to identify an employee it has designated to act on its behalf as a primary interface with Experian on systems access related matters. This individual shall be identified as the "Head Security Designate." The Head Security Designate can further identify a Security Designate(s) to provide the day to day administration of the Authorized Users. Security Designate(s) must be an employee and a duly appointed representative of the Company and shall be available to interact with Experian on information and product access, in accordance with these Experian Access Security Requirements. The Head Security Designate Authorization Form must be signed by a duly authorized representative of the Company. Company's duly authorized representative (e.g. contracting officer, security manager, etc.) must authorize changes to Company's Head Security Designate. The Head Security Designate will submit all requests to create, change or lock Security Designate and/or Authorized User access accounts and permissions to Experian's systems and information (via the Internet). Changes in Head Security Designate status (e.g. transfer or termination) are to be reported to Experian immediately.
2. As a Client to Experian's products and services via the Internet, the Head Security Designate is acting as the duly authorized representative of Company.
3. The Security Designate may be appointed by the Head Security Designate as the individual that the Company authorizes to act on behalf of the business in regards to Experian product access control (e.g. request to add/change/remove access). The Company can opt to appoint more than one Security Designate (e.g. for backup purposes). The Company understands that the Security Designate(s) it appoints shall be someone who will generally be available during normal business hours and can liaise with Experian's Security Administration group on information and product access matters.
4. The Head Designate shall be responsible for notifying their corresponding Experian representative in a timely fashion of any Authorized User accounts (with their corresponding privileges and access to application and data) that are required to be terminated due to suspicion (or actual) threat of system compromise, unauthorized access to data and/or applications, or account inactivity.

Designate

1. Must be an employee and duly appointed representative of Company, identified as an approval point for Company's Authorized Users.
2. Is responsible for the initial and on-going authentication and validation of Company's Authorized Users and must maintain current information about each (phone number, valid email address, etc.).
3. Is responsible for ensuring that proper privileges and permissions have been granted in alignment with Authorized User's job responsibilities.

4. Is responsible for ensuring that Company's Authorized Users are authorized to access Experian products and services.
5. Must disable Authorized User ID if it becomes compromised or if the Authorized User's employment is terminated by Company.
6. Must immediately report any suspicious or questionable activity to Experian regarding access to Experian's products and services.
7. Shall immediately report changes in their Head Security Designate's status (e.g. transfer or termination) to Experian.
8. Will provide first level support for inquiries about passwords/passphrases or IDs requested by your Authorized Users.
9. Shall be available to interact with Experian when needed on any system or user related matters.

By signing below, I acknowledge that I am an authorized representative for the company and as an end user of Experian products, will adhere to all of the above aforementioned requirements.

Raystown Realty Inc

Company Name

Signature

Burgess Smith Owner

Printed Name & Title

4/11/17

Date

Experian

Glossary

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

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

CREDIT SCORING SERVICES AGREEMENT

This Credit Scoring Services Agreement, ("Agreement"), dated: _____ ____, between _____ ("End User") Johnstown Credit Bureau, Inc._____ ("Provider")

WHEREAS, Provider is an authorized reseller of Experian Information Solutions, Inc. ("Experian"); and

WHEREAS, Experian and Fair, Isaac Corporation ("Fair, Isaac") offer the "Experian/Fair, Isaac Model", consisting of the application of a risk model developed by Experian and Fair, Isaac which employs a proprietary algorithm and which, when applied to credit information relating to individuals with whom the End User contemplates entering into a credit relationship will result in a numerical score (the "Score" and collectively, "Scores"); the purpose of the models being to rank said individuals in order of the risk of unsatisfactory payment.

NOW, THEREFORE, For good and valuable consideration and intending to be legally bound, End User and Provider hereby agree as follows:

1. General Provisions

A. Subject of Agreement. The subject of this Agreement is End User's purchase of Scores produced from the Experian/Fair, Isaac Model from Provider.

B. Application. This Agreement applies to all uses of the Experian/Fair, Isaac Model by End User during the term of this agreement.

C. Term. The term of this Agreement is a yearly, automatic self renewing contract. If End User wants to cancel, they shall submit, in writing, a thirty day notice for cancellation.

2. Experian/Fair, Isaac Scores

A. Generally. Upon request by End User during the Term, Provider will provide End User with the Scores.

B. Time of Performance. Johnstown Credit Bureau, Inc. will use reasonable methods to provide the Experian/Fair Isaac Model as expeditiously as possible and in a timely manner; provided, however, Johnstown Credit Bureau, Inc. will have no liability to End User for delays in providing such Model.

C. Warranty. Provider warrants that the Scores are empirically derived and statistically sound predictors of consumer credit risk on the data from which they were developed when applied to the population for which they were developed. Provider further warrants that so long as it provides the Scores, the Scores will not contain or use any prohibited basis as defined by the federal Equal Credit Opportunity Act, 15 USC Section 1691 *et seq.* or Regulation B promulgated thereunder. THE FOREGOING WARRANTIES ARE THE ONLY WARRANTIES PROVIDER HAS GIVEN END USER WITH RESPECT TO THE SCORES, AND SUCH WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, PROVIDER MIGHT HAVE GIVEN END USER WITH RESPECT THERETO, INCLUDING, FOR EXAMPLE, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. End User's rights under the foregoing warranties are expressly conditioned upon End User's periodic revalidation of the Experian/Fair, Isaac Model in compliance with the requirements of Regulation B as it may be amended from time to time (12 CFR Section 202 *et seq.*).

D. Release. End User hereby releases and holds harmless Provider, Fair Isaac and/or Experian and their respective officers, directors, employees, agents, sister or affiliated companies, and any third-party contractors or suppliers of Provider, Fair, Isaac or Experian from liability for any damages, losses, costs or expenses, whether direct or indirect, suffered or incurred by End User resulting from any failure of the Scores to accurately predict that a United States consumer will repay their existing or future credit obligations satisfactorily.

3. **Fees**. End User will pay Provider fees as agreed upon at time of initial membership/services agreement. These fees are subject to change at the discretion of the Provider and the End User will be notified of any changes at least thirty (30) days prior.

4. **Intellectual Property**

A. No License. Nothing contained in this Agreement shall be deemed to grant End User any license, sublicense, copyright interest, proprietary rights, or other claim against or interest in any computer programs utilized by Provider, Experian and/or Fair, Isaac or any third party involved in the delivery of the scoring services hereunder. End User acknowledges that the Experian/Fair, Isaac Model and its associated intellectual property rights in its output are the property of Fair, Isaac.

B. End User Use Limitations. By providing the Scores to End User pursuant to this Agreement, Provider grants to End User a limited license to use information contained in reports generated by the Experian/Fair, Isaac Model solely in its own business with no right to sublicense or otherwise sell or distribute said information to third parties. Before directing Provider to deliver Scores to any third party (as may be permitted by this Agreement), End User agrees to enter into a contract with such third party that (1) limits use of the Scores by the third party only to the use permitted to the End User, and (2) identifies Experian and Fair, Isaac as express third party beneficiaries of such contract.

C. Proprietary Designations. End User shall not use, or permit its employees, agents and subcontractors to use, the trademarks, service marks, logos, names, or any other proprietary designations of Provider, Experian or Fair, Isaac or their respective affiliates, whether registered or unregistered, without such party's prior written consent.

5. **Compliance and Confidentiality**

A. Compliance with Law. In performing this Agreement and in using information provided hereunder, End User will comply with all Federal, state, and local statutes, regulations, and rules applicable to consumer credit information and nondiscrimination in the extension of credit from time to time in effect during the Term. End User certifies that (1) it has a permissible purpose for obtaining the Scores in accordance with the federal Fair Credit Reporting Act, and any similar applicable state statute, (2) any use of the Scores for purposes of evaluating the credit risk associated with applicants, prospects or existing customers will be in a manner consistent with the provisions described in the Equal Credit Opportunity Act ("ECOA"), Regulation B, and/or the Fair Credit Reporting Act, and (3) the Scores will not be used for Adverse Action as defined by the Equal Credit Opportunity Act ("ECOA") or Regulation B, unless adverse action reason codes have been delivered to the End User along with the Scores.

B. Confidentiality. End User will maintain internal procedures to minimize the risk of unauthorized disclosure of information delivered hereunder. End User will take reasonable precautions to assure that such information will be held in strict confidence and disclosed only to those of its employees whose duties reasonably relate to the legitimate business purposes for which the information is requested or used and to no other person. Without limiting the generality of the foregoing, End User will take suitable precautions to prevent loss, compromise, or misuse of any tapes or other media containing consumer credit information while in the possession of End User and while in transport between the parties. End User certifies that it will not publicly disseminate any results of the validations or other reports derived from the Scores without each of Experian's and Fair, Isaac's express written permission.

C. Proprietary Criteria. Under no circumstances will End User attempt in any manner, directly or indirectly, to discover or reverse engineer any confidential and proprietary criteria developed or used by Experian and/or Fair, Isaac in performing the scoring services hereunder.

D. Consumer Disclosure. Notwithstanding any contrary provision of this Agreement, End User may disclose the Scores provided to End User under this Agreement (1) to credit applicants, when accompanied by the corresponding reason codes, in the context of bona fide lending transactions and decisions only, and (2) as clearly required by law.

6. Indemnification and Limitations

A. Indemnification of Provider, Experian and Fair, Isaac. End User will indemnify, defend, and hold each of Provider, Experian and Fair, Isaac harmless from and against any and all liabilities, damages, losses, claims, costs, and expenses (including attorneys' fees) arising out of or resulting from any nonperformance by End User of any obligations to be performed by End User under this Agreement, *provided that* Experian/Fair, Isaac have given End User prompt notice of, and the opportunity and the authority (but not the duty) to defend or settle any such claim.

B. Limitation of Liability. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, UNDER NO CIRCUMSTANCES WILL PROVIDER, EXPERIAN OR FAIR, ISAAC HAVE ANY OBLIGATION OR LIABILITY TO END USER FOR ANY INCIDENTAL, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES INCURRED BY END USER, REGARDLESS OF HOW SUCH DAMAGES ARISE AND OF WHETHER OR NOT END USER WAS ADVISED SUCH DAMAGES MIGHT ARISE. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF PROVIDER, EXPERIAN OR FAIR, ISAAC TO END USER EXCEED THE FEES PAID BY END USER PURSUANT TO THIS AGREEMENT DURING THE SIX MONTH PERIOD IMMEDIATELY PRECEDING THE DATE OF END USER'S CLAIM.

7. Miscellaneous

A. Third Parties. End User acknowledges that the Scores results from the joint efforts of Experian and Fair, Isaac. End User further acknowledges that each Experian and Fair, Isaac have a proprietary interest in said Scores and agrees that either Experian or the Fair, Isaac may enforce those rights as required.

B. Complete Agreement. This Agreement sets forth the entire understanding of End User and Provider with respect to the subject matter hereof and supersedes all prior letters of intent, agreements, covenants, arrangements, communications, representations, or warranties, whether oral or written, by any officer, employee, or representative of either party relating thereto.

IN WITNESS WHEREOF, End User and Provider have signed and delivered this Agreement.

Company: Rayburn Realty Inc

Name: Burgess Smith
Printed Name

Signature:

Title: Owner

Date: 4/11/17

Johnstown Credit Bureau, Inc.
2355 Bedford Street, Suite #4
Johnstown, PA 15904
Ph: 814-535-2513
Fax: 814-535-3364
E-mail: agorzelsky@creditrelatedinfo.com

FCRA Requirements

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

Although the FCRA primarily regulates the operations of consumer credit reporting agencies, it also affects you as a user of information. We have included a copy of the FCRA with your membership kit. We suggest that you and your employees become familiar with the following sections in particular:

§ 604.	Permissible Purposes of Reports
§ 607.	Compliance Procedures
§ 615.	Requirement on users of consumer reports
§ 616.	Civil liability for willful noncompliance
§ 617.	Civil liability for negligent noncompliance
§ 619.	Obtaining information under false pretenses
§ 621.	Administrative Enforcement
§ 623.	Responsibilities of Furnishers of Information to Consumer Reporting Agencies
§ 628.	Disposal of Records

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

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

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

In addition to the Federal Fair Credit Reporting Act, other federal and state laws addressing such topics as computer crime and unauthorized access to protected databases have also been enacted. As a prospective user of consumer reports, we expect that you and your staff will comply with all relevant federal statutes and the statutes and regulations of the states in which you operate.
We support consumer reporting legislation that will assure fair and equitable treatment for all consumers and users of credit information.

Signature/Title

4/11/17
Date

Membership Application

JOHNSTOWN CREDIT BUREAU, INC.
2355 BEDFORD STREET SUITE #4
JOHNSTOWN, PA 15904
PH: (814) 535-2513 FAX: (814) 535-3364

Date of Application: 4/6/17

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

General Individual/Company Information

Individual/Company Name: _____

Years in Business 36 yrs _____ mos.

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

Do you have any other company name(s) or dba? ☑ **Yes** ☐ **No** **If Yes**, please list: ANTHONY & ASSOCIATES

Company website(s): www.RAYSTOWNREALTY.com

Contact Person: Burgess Smith Email: burgess@raystownrealty.com

Physical Street Address (**no P.O. box numbers, please**): 310 2nd Stk

City: Huntingdon State: Pa ZIP: 16652 How Long? 25+/- yrs _____ mos.

Phone: (814) 643-5054 Fax: (814) 643-4774 Is this a **residential** address? ☐ **Yes** ☑ **No**

Previous Address: _____

City: _____ State: _____ ZIP: _____ How Long? _____ yrs _____ mos.

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

Principal of the Company

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

Principal name: Burgess Smith

Title or Position: _____ Phone: ( ) _____

Residential Street Address: _____

City: _____ State: _____ ZIP: _____

Business Information

(Please tell us about your company.)

Type of Business: Real Estate Sales Do you need a Purchase Order? ☐ **Yes** ☑ **No** PO# _____

Do you have an **Investigation License**? ☐ **Yes** ☑ **No** **If Yes, please provide a copy with this application.**

Estimated # of Credit Reports you will access monthly: 1 per year

How will you access the Credit Reports? ☑ **Personal Computer** ☐ **Credit Terminal** ☐ **CPU-CPU** ☑ **Phone/Fax**

Do you already have a credit reporting software package? ☐ **Yes** ☑ **No** If **Yes**, what is the name? _____

Does your company qualify for sales tax exemptions? ☐ **Yes** ☑ **No** If **Yes**, please provide proof.

Permissible Purpose/Appropriate Use (Application will not be processed unless this information is provided.)

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

This section MUST be completed.

to qualify ~~Applicants~~ Tenants for prior to signing lease

I have 2 Rental properties

The following applies to consumer credit products (i.e. Consumer Credit Reports, Business Owners Profile, and Small Business Intelliscore):

I have read and understand the "**FCRA Requirements**" notice and "**Access Security Requirements**" and will take all reasonable measures to enforce them within my facility. I certify that I will use the Experian product information for no other purpose other than what is stated in the Permissible Purpose/Appropriate Use section on this application and for the type of business listed on this application. I will not resell the report to any third party. I understand that if my system is used improperly by company personnel, or if my access codes are made available to any unauthorized personnel due to carelessness on the part of any employee of my company, I may be held responsible for financial losses, fees, or monetary charges that may be incurred and that my access privilege may be terminated. **Any invoice that is thirty (30) days past due, will be assessed a 1.5% late fee.**

In order to cooperate with other business and professional people in the confidential dissemination of credit information, the undersigned (hereinafter referred to as the ***Applicant)*** petitions the Johnstown Credit Bureau (hereinafter referred to as the ***Credit Bureau***) for the use of its services upon the basis outlined above, and if accepted by said Credit Bureau as a member or subscriber, agrees that the following shall constitute a service contract between the Applicant and the Credit Bureau.

THE APPLICANT CERTIFIES AND AGREES:

To pay monthly membership fees in accordance with the amount(s) listed above. Membership shall entitle the Applicant to services provided by the Credit Bureau according to the schedule of charges now or subsequently established by the Credit Bureau.

The Applicant will comply with all the provisions of the Public Law 91-508 (Fair Credit Reporting Act) and all other applicable statutes, both state and federal.

That each time a request for information or a credit report is made of the Credit Bureau, the Applicant's representative authorized to make such a request will use the information or report solely for a permissible purpose, namely:

(A) In connection with a credit transaction involving the consumer on whom the information is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer; or

(B) For employment purposes; and Applicant agrees to make the employment certification below; or

(C) For screening of prospective tenants for rental properties (tenant screening); or

(D) In connection with a legitimate business need for the information in connection with a business transaction initiated by the consumer or to review an account to determine whether the consumer continues to meet the terms of the account; and the Applicant agrees to identify to the Credit Bureau each request at the time such report is ordered, and to certify the legitimate business need for such report.

Reports on employees will be requested only by the Applicant's designated representatives. Employees will be forbidden to attempt to obtain reports on themselves, associates, or any other person except in the exercise of their official duties.

That each time a request for information or a credit report is made of the Credit Bureau for employment purposes it will comply with s604 of the FCRA, namely: (1) the consumer has been given a clear and conspicuous written notice, in advance (in a document that consists solely of the disclosure), that a consumer report may be requested for employment purposes; (2) the consumer has authorized the Applicant, in writing, to procure the report; (3) the information in the consumer report will not be used in violation of any applicable federal or state equal employment opportunity law or regulation; (4) before taking adverse action, in whole or in part on the report, Applicant will provide the consumer a copy of the report and a description of the consumer's right under the FCRA.

(Public Law 91-508 provides that any person who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses shall be fined under Title 18 of the United States Code, or imprisoned not more than two years, or both)

Applicant may discuss information received from Credit Bureau with the consumer in the event Applicant declines or takes adverse action regarding the consumer. In the event of disclosure to the consumer by Applicant, the Credit Bureau shall be held harmless from any liability, damages, cost or expense including reasonable attorney's fees resulting therefrom. The Credit Bureau shall not be liable in any manner whatsoever for any loss or injury to Applicant resulting from the obtaining or furnishing of such information and shall not be deemed to have guaranteed the accuracy of such information, such information being based, however, upon reports obtained from sources considered by the Credit Bureau to be reliable.

Credit Bureau shall have the right to audit records of the Applicant that are relevant to the provision of services set forth in the agreement. Applicant further agrees that it will respond within a requested time frame for information that is requested by Credit Bureau's consumer reporting vendor regarding information provided by such Credit Bureau. Applicant understands that such Credit Bureau may suspend or terminate access to the Credit Bureau's information in the event the Applicant does not cooperate with such an investigation.

IT IS MUTUALLY AGREED that this service contract, if accepted by the Credit Bureau, shall remain in force and effect for one (1) year and thereafter, from year to year, on the same basis as set forth herein until written notice of cancellation shall be given by either party at least thirty (30) days prior to cancellation. It is further agreed, however, that if Applicant is delinquent in the payment of charges, or is guilty of violating the terms of this contract, the Credit Bureau may, at its election, discontinue providing service to the Applicant and cancel this contract immediately by written notice to the Applicant.

IT IS FURTHER MUTUALLY AGREED that the Credit Bureau and the Applicant shall be liable to any third party claimant for its own act of negligence with regard to the performance of its duties hereunder, and each shall indemnify and hold harmless the other for and from all such third party claims arising on account of its act of negligence, or on account of its failure to perform any of its obligations hereunder, and any cost or expense, including reasonable attorney's fees, incurred by the other in connection therewith.

Burgess Smith / Raystown Realty Inc
Individual/Company Name

Burgess Smith — Owner
Type or Print Name of Owner or Officer — Title

X [signature]
Authorized Signature — Date 4/11/17

Revised 10/98

DO NOT WRITE BELOW THIS LINE – FOR OFFICE USE ONLY

Approved By: _____ **Date:** _____

Printed Name & Title

Subscriber Number & Password