703-494-5932 Office
703-494-5783 Fax
Marie@RegorRecovery.com

RegorRecovery.com
P.O. Box 498
Woodbridge, VA 22194

Regor Recovery LLC

COMPLIANCE AND OPERATIONS MANUAL

Table of Contents

Foreword

With the passage of the Dodd-Frank Consumer Protection Act, and the creation of the Consumer Financial Protection Bureau (CFPB) under that federal law, the lending community and those who are defined as "Business Associates" under the Gramm-Leach-Bliley Act (GLBA) are facing a new era of federal regulation and compliance requirements. The CFPB is taking an aggressive and proactive approach in

implementing and enforcing the new regulations, and those who have not met these new compliance requirements are facing long-term litigation and huge fines for noncompliance.

As "Business Associates," collateral recovery specialists will face the challenge of making their companies "unassailable" in order to avoid costly litigation and ensure long-term success under these new regulations and compliance demands. Meeting these demands will require a new and concerted effort on the part of collateral recovery agency owners and their employees, and we believe those who accept the challenge will benefit over the long term.

The Gramm-Leach-Bliley Act (GLBA)

Protecting Nonpublic Personal Information (NPPI)

This federal law provides the parameters for the protection and disclosure of Nonpublic Personal Information (NPPI) to nonaffiliated third parties by financial institutions. **In the GLBA Section 501(a): Protection of nonpublic personal information,** it states, "It is the policy of the Congress that each financial

institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."

Associated Investigators of Tampa, Inc. recognizes that, as collateral recovery specialists, we are "Business Associates" (direct representatives) of those lending institutions we service and are therefore subject to the requirements of this federal law. As business associates of our lender clients we are not considered to be nonaffiliated third parties and therefore our lender clients are permitted to provide us with certain NPPI necessary to service their repossession assignments. **We therefore agree that we will not divulge this NPPI to a <u>nonaffiliated third party</u> during the performance of our services to our clients.**

The GLBA defines NPPI to include but not be limited to:
Social Security number
Taxpayer Identification number
Bank Account numbers, including checking, savings and trust accounts, loan accounts, medical savings account or any other account numbers held in a financial institution, etc.
Credit card information, including card number(s) in whole or in part, expiration date and cardholder name and address.
Telephone numbers (including unlisted, nonpublished and wireless)
Driver's license number
Medical information, including but not limited to: doctor name(s) and medical claims, insurance claims, prescriptions, treatment(s) or diagnoses, and any related personal medical information
Credit bureau records
Employment records, including income information
Date of birth
Addresses not normally accessible to the public
Any derogatory information
Child support information
Bankruptcy information
Financial information, including bank balances, payment amounts, past due amounts, etc.

In order to fulfill the requirements for protecting NPPI, the owner of Associated Investigators of Tampa, Inc. has made the following position appointments:
<u>Note</u>: Agency owner shall determine the responsibilities of each Designated Appointee and may appoint himself/herself to any, or all, of these positions.

Data Security Specialist: (name)
Security Officer: (name)
Human Resources Officer: (name)
Training Officer: (name)

Procedures for Security and Protection of NPPI

Associated Investigators of Tampa, Inc. has adopted the following procedures for the security and protection of NPPI.

Clean Desk Policy:

1. Only files that are being actively worked should be on the employee's desk. Only the file that is being worked should be open.
2. All other files being actively worked should be secured in a folder with no identifying information visible.
3. Employees shall not leave NPPI, sensitive papers or documents in open view when away from their work stations.
4. At the end of the day the **Designated Appointee** shall ensure that no files containing NPPI are left on the desk.

A. Only NPPI that is necessary for completing an assignment shall be taken into the field. This information shall be contained on a laptop computer with secured passwords and shall be shredded [deleted?] as soon as possible after use. Unless necessary, no paperwork shall be taken into the field except for impounds and seizures.

Note: To reduce the possibility of a Wrongful Repossession, when a field assignment is closed the office staff shall immediately close the assignment in the database and contact field agent to reconfirm the close.

B. All paper documents or files, including CDs, floppy disks, zip drives, flash drives, tapes and backups, containing NPPI and not being actively worked shall be stored in a designated, secured and locked area.

C. File cabinets containing NPPI shall be stored in a designated, secured and locked area.

D. At the end of the day, employees shall secure files, log off their computer, and lock their file cabinets and office. The **Designated Appointee** shall ensure that all files, computers and storage areas are secure.

E. Access keys/codes shall be given only to employees with an authorized need. Employees entering areas where sensitive files are kept shall document the visit.

F. Visitors who, for legitimate reasons, enter areas where sensitive files are maintained must be escorted by an authorized employee of **Associated Investigators of Tampa, Inc. .**
G. No visitor shall be given entry codes/keys or be allowed unescorted access.

Security and Protection of Electronic Records

A. **General network security**
   (a) NPPI shall not be stored on any computer with an Internet connection unless essential for conducting business.
   (b) NPPI sent to third parties over public networks shall be encrypted.
   (c) NPPI stored on the computer network or on disks or portable storage devices used by employees shall be encrypted.
   (d) NPPI may be transmitted internally using approved email procedures and must be encrypted.
   (e) NPPI sent externally shall be encrypted and password-protected, and must be sent only to authorized recipients. Additionally, a statement such as the following shall be included in the email: **"This message may contain confidential and/or proprietary information and is intended for the person/entity to whom it was originally addressed. Any use by other(s) is strictly prohibited."**
   (f) Anti-virus and anti-spyware programs shall be run daily on individual computers and network servers.
   (g) When receiving or transmitting credit card information, other sensitive financial data or health information, Secure Sockets Layer (SSL) or another secure connection shall be used to protect the information in transit.

B. **Password management:**
   (a) Access to NPPI shall be controlled using "strong" passwords. Employees shall choose passwords with a mix of letters, numbers and characters. User names and passwords must be different and passwords shall be changed at least monthly.
   (b) Passwords shall not be shared or posted near workstations.
   (c) Password-activated screen savers shall be used to lock employee computers after a period of inactivity.
   (d) When installing software, vendor-supplied default passwords shall immediately be changed to a more secure "strong" password.

C. **Laptop security:**
   (a) Laptop use is restricted to employees who need them to perform their job responsibilities.

(b) When using laptops, a secure wireless connection must be used. Wi-Fi hotspots are not secure in public places.
(c) If NPPI does not need to be stored on a laptop, it shall be deleted with a "wiping" program that overwrites data.
(d) Laptops shall be stored in a secured area.
(e) Authorized laptop users will have access to NPPI but shall not store such information on laptops.
(f) Laptops containing NPPI shall be encrypted and configured so users cannot download software or change security settings without approval from the company's IT specialist(s).
(g) Laptops shall be configured with an "auto-destroy" function so that data on a computer that is reported stolen will be destroyed when the computer is used to try to access the Internet.
(h) Employees must not leave a laptop visible in an automobile, residence or hotel luggage stand, or in "checked" luggage at an airport unless directed to do so by airport security.
(i) Laptops or paper product information must not be left in a vehicle at night in order to protect against theft.
(j) Off-lease computers shall have hard drives completely wiped clean and copiers that are being returned shall have all NPPI completely removed.

D. **Firewalls:**

(a) A firewall shall be used to protect computers from hackers while connected to the Internet.
(b) The computer network shall have a "border" where it connects to the Internet. Access controls shall be set to allow only trusted employees with an authorized business need to access the network.
(c) Additional firewalls shall be used to protect computers containing Personally Identifiable Information.
(d) Firewalls shall be reviewed periodically.

Disposal of NPPI

A. When documents containing NPPI are discarded, they shall be placed in a locked shred bin or immediately shredded using a mechanical cross-cut shredding device approved by the Department of Defense.
B. Locked shred bins shall be labeled as **Confidential Paper Shredding and Recycling Bins.**
C. When disposing of computers and portable storage devices, a disk-wiping utility program approved by the Department of Defense shall be used.

D. Any CD-ROM, DVD-ROM, floppy disk or flash drive shall be disposed of by shredding, incinerating or punching holes in the device.

Copier Data Security:

The **Designated Appointee s**hall check with the manufacturer, dealer or servicing company for options on securing the hard drive and, if necessary, will work with skilled technicians in securing the hard drive.

Security Practices of Contractors and Service Providers

Associated Investigators of Tampa, Inc. shall exercise appropriate and effective oversight of contractors and service provider arrangements, including the following:

A. It shall ensure that the activities of contractors and service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risks of identity theft and to protect NPPI.
B. A contractor or service provider that maintains its own Identity Theft Prevention Program, consistent with the guidelines and requirements of the federal Red Flags Rules, 16 C.F.R., Part 681, and validated by appropriate due diligence, may be considered to be meeting these guidelines and requirements.
C. Any specific requirements shall be addressed in appropriate contract arrangements.
D. Contractors and service providers must notify (recovery agency's) **Designated Appointee** of any security incidents, regardless of whether or not such incidents led to actual compromise of data.
E. (Recovery agency's) **Designated Appointee** shall ensure that the activities of contractors and service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risks of identity theft.

Disaster Preparedness Planning

Disasters come in many forms, including but not limited to: fire, flood, hurricane, tornado, technological emergencies, etc.

In order to resume operations quickly in the event of a disaster or catastrophic event, Associated Investigators of Tampa, Inc. has adopted and put in place the

following disaster planning procedures and policies for responding to occurrences including but not limited to those mentioned above:

Protection of Business and Sensitive Data:

The following backup plan has been created for the retention and protection of all business and sensitive company data:

A. At the close of business Monday through Thursday, incremental backup of all servers.
B. At the close of business each Friday, a full backup of all servers.
C. At the completion of the full backup each Friday, all backups shall be taken by recovery agency owner or **Designated Appointee** to a secured, remote location. Sixty (60) days of data shall be maintained at the secured, remote location.
D. Only the recovery agency owner or **Designated Appointee** shall have access to the secured, remote location where backup data is stored.
E. The recovery agency owner or **Designated Appointee** shall monitor the storage and/or removal of backed up data and shall ensure that applicable access controls are in place and adhered to.
F. Backup procedure tests shall be done at least annually to ensure that data is available for retrieval if necessary.

Notification of a Disaster or Catastrophic Event:

Associated Investigators of Tampa, Inc. has approved the following procedures for maintaining contact information for all persons who must be contacted in the event of a disaster or catastrophic event, including:

A. Individual(s) at backup data system(s) where business and sensitive data is stored.
B. Individual(s) who maintain Information Systems.
C. Vendors who have a need to know that a disaster or catastrophic event has occurred.
D. Workforce personnel who have a need to know that a disaster or catastrophic event has occurred.
E. Locate available and applicable work areas and alternate systems that can be used while company locations and normal information systems are not available.
F. All immediate steps available to restore normal operations at company location(s).

Putting the Plan into Action:

In the event a disaster or catastrophic event should occur the following procedures shall be immediately taken:

A. Contact all individuals listed under **Notification of a Disaster or Catastrophic Event.**
B. Secure all sites of company operations by live security and maintain live security wherever business and sensitive data is located.
C. Ensure that the location of backup data continues to be secured.
D. Retrieve all lost data that can be located and ensure that data is secured in a secure, remote location by the company owner or designated company security officer.

Disaster Preparedness Procedures:

1. Check work vehicles for fuel. Make sure all work vehicles are filled to capacity.
2. Fill reserve fuel tanks.
3. Work vehicles should be parked inside the storage lot away from fence.
4. Check tire pressure and have spare tires on hand.
5. Check cell phones for battery life.
6. Have flashlights and extra batteries.
7. Make sure each employee has phone numbers for management and/or co-workers.
8. Make sure each employee has rain gear.
9. Make sure nonperishable food and water is accessible.
10. Check shop stock material, including oil, belts, hoses, tools, wiper blades, duct tape, tarp, battery charger, rope, generator, trash bag, etc.
11. Cover all windows with plywood or other protective material.
12. Have wet/dry vacuum on hand.
13. Have digital cameras on hand with two backup batteries.
14. Forward business phone to management.
15. Unplug computers and electronic components and waterproof them.
16. Raise all electronics off the floor and onto higher ground.
17. Begin to track storm and estimated landfall locations and time.
18. Maintain telephone numbers for post-disaster services such as utilities, debris removal, computer technician, labor centers, etc.

Storage Facility:

1. Transport as many vehicles to auction ASAP.
2. Expedite removal of vehicles scheduled for transport.

3. Make sure all vehicles are on highest ground in the storage facility and away from trees.
4. Remove all debris and potential hazards from storage facility, such as tree limbs, wood or other loose materials.
5. Any loose materials that cannot be removed should be tied down or otherwise secured.

Post-Disaster:

In a paperless environment, work can commence as soon as it is safe to do so under the following procedures:

1. Employees should check with management regarding job responsibilities. It may be necessary for employees to work from their residence until the office facilities are safe.
2. Designate specific employees for post-disaster tasks; for example, designate specific employee(s) to provide updates to staff, and to call utilities, debris removal service, computer technician, etc.
3. Provide designated employee(s) with telephone numbers for post-disaster services.

Reviewing the Plan:

Associated Investigators of Tampa, Inc. shall review its Disaster Preparedness Plan on a regular basis to ensure it remains effective.

The Consumer Financial Protection Bureau (CFPB)

The preamble of the CFPB Bulletin 2012-03 states the following:
"The Consumer Financial Protection Bureau (CFPB) expects supervised banks and nonbanks to oversee their business relationships with service providers in a manner that ensures compliance with Federal consumer protection law, which is designed

to protect the interests of consumers and avoid consumer harm. The CFPB's exercise of its supervisory and enforcement authority will closely reflect this orientation and emphasis."

The CFPB expects supervised banks and nonbanks to have an effective process for managing the risks of service provider relationships. The CFPB will apply these expectations consistently, regardless of whether it is a supervised bank or nonbank that has the relationship with a service provider.

To limit the potential for statutory or regulatory violations and related consumer harm, supervised banks and nonbanks should take steps to ensure that their business arrangements with service providers do not present unwarranted risks to consumers.

In the bulletin, the CFPB clearly defines a Service Provider as:
"Service provider is generally defined in section 1002(26) of the Dodd-Frank Act as '**any person that provides a material service to a covered person in connection with the offering or provision by such covered person of a consumer financial product or service.'"**

More simply put, a Service Provider is a provider of services that holds a consumer's Nonpublic Personal Information (NPPI). It is abundantly clear that those who service self-help repossessions are considered Service Providers under the CFPB.

Following are specific procedures that Associated Investigators of Tampa, Inc. has adopted for handling complaints as required by the CFPB. **Form G,** in the **Forms Section,** is a specially designed **Complaint Handling Checklist Form** that meets all CFPB requirements and guidelines for handling customer complaints.

CFPB Customer Complaints Procedures

An effective customer complaint system is an essential part of any business as it indicates to our customers that quality service is a vital part of what we do. A complaint handling system is an organized way of responding to, recording, reporting and using

complaints to improve service to our customers. It includes procedures for customers to make complaints and guidelines for staff to resolve complaints, and provides information to managers and staff that they can use to prevent customer dissatisfaction in the future.

An effective customer complaint handling system is an essential part of providing quality service. It is a measure of customer satisfaction. It provides positive feedback about aspects of our service that work well and is a good source of information for improvement.

An effective complaint system creates a second chance to provide service and satisfaction to dissatisfied customers, identifies area(s) that need improvement and provides opportunities to strengthen our standing in the industry.

Quality customer service consists of doing the job right and providing appropriate service at the outset. If and when things go wrong in the process, they can be made right and quality service delivered. Quality service and making things right are the hallmarks of our organization.

Customer complaints represent the experience and feelings not just of the complainants but also of others in similar circumstances who chose not to complain. Customer complaints should be acted on in two ways. First, the specific grievance must be resolved if at all possible. Second, information about the nature of the complaint must be kept to provide feedback about our system and processes. Often, complaints are an early warning of concerns held by a larger percentage of customers who experienced similar dissatisfaction but had not bothered to complain.

Facts about Handling Complaints:

1. It costs six times as much to attract a new client as it does to keep an old one.
2. A typical dissatisfied client will tell eight to 10 people about his/her problem.
3. Seven of 10 complaining clients will do business with you again if you resolve the complaint in their favor.
4. If you resolve the complaint on the spot, 95% will do business with you again.
5. Of those clients who stop doing business with you, 65% do so because of an attitude of indifference on the part of your company or a specific individual.

Notification Procedures:

Should (name of collateral recovery agency) personnel, including contractors and service providers, become aware of any threatened, potential or actual incident concerning the unauthorized use of, or access to, confidential information, the following steps and procedures shall be followed:

A. The person who discovers the incident or potential incident shall contact one of the following owners of (name of collateral recovery agency):

Note: List names and telephone numbers of all collateral recovery agency owners.

B. When the call/report is received by one of the (collateral recovery agency owners), the following information shall be logged:

(a) Caller's name and contact information
(b) Time of call
(c) Nature of the incident
(d) Description of equipment and name of person(s) involved
(e) How the incident was detected
(f) When the event first was noticed

C. The notified owner then shall contact, by email and telephone, the response team comprised of all owners and department managers, and (the recovery agency individual designated as responsible for training). The team shall determine a response strategy. The following information shall be documented:

(a) How the incident was discovered
(b) How the incident occurred, whether via email, firewall, physical security beach, etc.
(c) Where the attack came from, such as an IP address and other related information about the attacker
(d) What response plan was devised
(e) Whether the response plan was effective

D. Evidence will be preserved by creating copies of logs, emails and other documentable communication. Lists of witnesses shall be recorded and digital recordings of security cameras shall be preserved if necessary.

E. Notification shall be provided to affected lienholders/clients, as well as to appropriate external agencies such as law enforcement.

F. The response will be reviewed and, if appropriate, policies and procedures updated. The response team shall take preventative measures to ensure such incidents will not happen again.

G. Random reviews and testing shall be done at least annually to help ensure appropriate procedures are followed.

Complaint Handling:

The majority of complaints should be handled immediately by the frontline staff. When handling a complaint, the staff must:

- Understand a complainant's needs
- Build rapport
- Listen effectively
- Demonstrate empathy
- Ask the right questions

Guidelines that the staff should always keep in mind when dealing with a customer complaint are:

- Treat complainants respectfully, pleasantly and professionally at all times
- Give your names, greet the person courteously and ask in a positive manner how you can help
- Listen to what the person has to say
- Use good listening skills
- Seek clarification of any points that are not clear and do so in a nonjudgmental way
- Provide any relevant information that will assist the complainant to better understand the decision or action
- Show empathy
- Try to meet any reasonable request that would solve the problem
- Offer solutions that can be delivered
- Take responsibility for solving the problem on the spot
- Handle complaints quickly, within established timeframes

- Log the complaint and action taken for future analysis

If the customer is not satisfied by the response received from the initial staff member, the complaint should be sent to the next level for review and handling.

At this level, the reviewer should contact the complainant to clarify the complaint and the outcome sought, and to explain the investigative procedure. In addition, the reviewer should gather all relevant evidence and discuss the complaint with the relevant parties. After review, a report should be drafted and kept in the file. The complainant should be contacted to explain the results of the investigation and what, if any, action will be taken consistent with, or supplemental to, the prior action.

Best Practices

As stated in our introduction, in order to ensure that the collateral recovery agency is "unassailable" and all compliance issues are met effectively, it is imperative that hiring and training figure prominently in the business plan. In addition, office and storage facilities should meet accepted industry standards. Associated Investigators of Tampa, Inc. has addressed those concerns and adopted the following procedures:

Hiring: Pre-Employment Screening:

The initial hiring interview should include the applicant being advised - and required to sign an affidavit of understanding and agreement - that the background check will be accomplished in accordance with the Fair Credit Reporting Act (FCRA), the Americans with Disabilities Act (ADA), the Equal Employment Opportunity Commission (EEOC) and all other applicable federal and state laws and local requirements. In order to comply with the EEOC, the applicant should be advised that the entire background check will be considered in making a hiring decision, but that any criminal record will carry significant weight if it shows that the applicant has a record of crimes against persons, domestic abuse, drug addiction, pedophilia, etc. The applicant should also be advised, and the affidavit should state, that **any and all documents** acquired in the interview process may be considered in determining whether the applicant will be hired.

All applications, documents, affidavits, interviews, etc. shall be placed in a secured and locked area with limited access/authority to enter the area and inspect those documents.

1. Check references as to training and professional certification, other professional credentials and overall competency of the applicant.
2. Check driver's license records. Accepted industry standards do not allow repossession activity by individuals operating a tow truck with a suspended or revoked driver's license, and do not recognize the use of nonemployees assisting in the self-help repossession process.
3. Check criminal history to make sure the applicant is not a convicted felon, drug or alcohol abuser or sex offender, does not have a propensity for violence and is mentally competent. An applicant who has been convicted of a crime against persons, such as assault, battery, domestic violence, etc., should not be considered for employment as a Field Recovery Specialist.
4. Require the applicant to be professionally certified through a nationally accepted collateral recovery certification program or provide proof of such certification. In considering an in-house program, also consider that courts generally lend considerably more credibility to nationally recognized, independent programs. Further, in a profession deemed by courts across the country as involving "inherent" risks, it is not unreasonable to require those who service self-help repossession assignments to be subject to at least

annual Continuing Education. The certification program should include but not be limited to the following subjects:

A. Fair Debt Collection Practices Act (FDCPA)
B. Gramm-Leach-Bliley Act (GLBA)
C. Telephone Records Privacy Protection Act (TRPPA)
D. Servicemembers Civil Relief Act (SCRA)
E. Uniform Commercial Code (UCC)
F. Breach of the Peace
G. Defensive Driving
H. Ethics, Professional Conduct and Communication
I. Crimes Against Persons and Property
J. The Collateral Recovery Process

5. Confirm that the applicant has a valid repossessor's license if it is required by the state where the applicant will be servicing repossession assignments.

Training:

1. Upon hiring, the employee should be supervised in the field by a professionally trained and certified supervisor until the supervisor is satisfied that the employee understands the various federal and state laws, and local ordinances that impact the self-help repossession process where the employee will be servicing those assignments. In addition, the employee must demonstrate that he/she: has a sufficient understanding of what constitutes a Breach of the Peace; has adequate communication skills when confronting the debtor(s) and/or bystander(s); knows when to stop the repossession process and leave during a confrontation with the debtor(s) and/or bystander(s); and knows to immediately document any confrontation in writing on the company's Incident Reporting Form.
2. Make sure the employee understands that he/she cannot threaten, intimidate or use force or profanity while communicating with debtor(s) and/or bystander(s) during the repossession process.
3. Make sure the employee understands that he/she cannot enlist the assistance of law enforcement in a self-help repossession.
4. Make sure the employee understands the process, and recognizes the duty to follow proper procedures in inventorying and protecting personal

property and Nonpublic Personal Information contained in the repossessed collateral.

5. Make sure the employee is property trained in tow truck use so that repossessed collateral is not damaged while being towed.
6. Make sure the employee understands that accepted industry standards prohibit nonemployees, untrained or under-trained individuals and minor children from assisting in the physical act of repossession. Such individuals increase the potential for added risks and volatile situations.
7. Make sure the employee understands the definition of Nonpublic Personal Information (NPPI) and that, under no circumstances, is he/she allowed to divulge NPPI to a third party.
8. Make sure the employee understands that he/she is to take only information to the field that has been provided to them by designated office staff.
9. Make sure the employee understands the importance of a timely and accurate condition report.
10. Make sure the employee understands a comprehensive status report is second in importance only to the actual repossession.
11. The certified supervisor shall ensure the employee signs all training forms as the specific training areas are completed.
12. Institute an ongoing training policy that requires Continuing Education at least once each year. Every Continuing Education course should include Defensive Driving and Breach of the Peace. The employee should sign an affidavit that he/she has completed such training.
13. **The certified supervisor should record the employee's progress in writing and provide this documentation to the Training Officer, who shall place such reports in the employee's secured personnel file**

Collateral Condition Reports:

- The condition report shall be completed within six (6) hours after the collateral has been secured at the recovery agency storage facility.
- Take multiple pictures of the recovered unit, especially after-market equipment, specialty equipment and damage.

- Vehicle windows and sunroof, if applicable, need to be closed to protect the interior.
- Vehicle with a damaged window or sunroof should have a tarp draped over it to protect the interior.
- Complete and reaffirm the condition report is accurate and legible.
- Place any vehicle keys in the designated, secured area.

Personal Property Inventory Processing and Protection:

The inventory, protection and return of personal property are addressed in the following case law:

1. **Nadalin . Automobile Recovery Bureau, Inc., 169 F. 3d 1084 U.S. Court of Appeals, Seventh Circuit IL (1999)** states, in part, that the Security Agreement between the creditor and the debtor authorized the creditor to take **"any goods found in the vehicle not covered by this agreement at the time of repossession, provided that the lender make reasonable efforts to return them to the debtor after repossession."** The performance of this contractual duty required **inventorying, storage and notice of the personal property.** This case also confirms the legality of the repossessor to charge a **reasonable** fee for the storage and protection of personal property.
2. **GMAC v. Vincent, 523 83 P. 2d 539 183 OK 547 Sup. Ct. (1938)** states, in part, that the seller may take possession of any property in the vehicle at the time of repossession, **"and hold same temporarily for the purchaser without liability on the part of the seller but the failure of the Defendants to account to the Plaintiff for the property upon his demand therefore would constitute a wrongful exercise of dominion over the same. Accordingly, Defendants would be liable to Plaintiff for the actual case value of the personal property which was in the automobile at the time of the taking and for which Defendants failed to account to Plaintiff."**

- Contractor's relationship to personal property is that of a "bailee," and Contractor shall therefore make all reasonable efforts to safely store and protect all personal property contained in or on the recovered collateral in accordance with applicable law and compliance procedures. Contractors are

also responsible to ensure that the debtor is properly and promptly notified as to the procedures for redeeming personal property.

- The inventory shall be performed, in writing, by recovery agent who recovered the property upon securing the collateral at the storage facility to ensure that a "chain of custody" is maintained. The recovery agent shall sign and date the inventory, attach an identification tag to the personal property container and place the personal property in the designated, secured storage area.
- If NPPI is found inside the collateral, place all NPPI in a smaller bag within the bag containing the personal property so that, in the event the debtor does not reclaim the personal property, the NPPI can be shredded or otherwise disposed of properly.
- Personal property shall be properly secured, organized and easily identified.

Hostile Debtor Policy

It is important for the recovery agency to have procedures for handling hostile debtors in the office, over the telephone and especially in a confrontational situation involving the physical act of repossession. Associated Investigators of Tampa, Inc. has adopted the following procedures to help control and mitigate the risks from a hostile debtor.

Office:

The debtor, debtor's representative or individuals accompanying a debtor should never be allowed in the office area. If possible, an area of the office shall

be sealed off from the actual office area with an opening for the debtor to speak with office staff. If this is not possible, other arrangements shall be made to ensure that the debtor does not have access to the office and that no physical contact is possible between the debtor and office staff. Should the debtor be accompanied by any other person, office staff must not discuss the account in the presence of the accompanying parties and must not engage in a verbal or physical altercation. If the debtor or any accompanying party becomes hostile ask them to leave immediately. If they refuse, call 911 and request assistance. Try to be sure the debtor or accompanying party hears the call being made to 911 as this will, in most situations, convince the debtor and accompanying party of the seriousness of their actions, at which point they will usually leave without further disturbance. If the debtor and accompanying party leave before police arrive, provide a complete statement, and descriptions of the debtor and accompanying party, and request the debtor and accompanying party be given a **Trespass Warning.** Office staff should then complete an Incident Report Form to be maintained in the debtor's file with a copy also provided to the client..

Telephone:

When a debtor calls, office staff should be courteous and especially alert to any signs of hostility. Any hostile remarks by the debtor should be countered with courteous, professional yet firm responses. Explain to the debtor that it is standard procedure to immediately report to law enforcement any attempt at misbehavior on his/her part while at your office. If the debtor ignores your warnings and begins to display hostility while at your office, follow the instructions described in Office procedures.

Field Activity:

In the event a Field Recovery Specialist encounters hostility during the physical repossession process, he should attempt to use his communication skills to defuse the confrontation. The Field Recovery Specialist shall explain in a nonthreatening manner that if the debtor refuses to allow the repossession to take place the creditor has the right to have law enforcement take the collateral by court order. If the Field Recovery Specialist cannot successfully obtain the debtor's consent to the repossession, he/she shall immediately cease attempts to repossess the collateral and then provide a comprehensive status report to the office and to the client.

Under no circumstance shall the Field Recovery Specialist request the assistance of a law enforcement officer to assist in the repossession.

Storage Facilities, Office and Equipment Security

Storage Facilities:

- 6-foot-high chain link fence with barbed wire at a minimum.
- Gate must be locked at all times when not in use.
- There should be no holes or breaks in the fence.
- Motorcycles and ATVs should be locked inside a secure storage facility. If not possible, each vehicle should be chained to further protect the asset from theft.
- Video cameras should be used to deter theft and to record events in the storage lot and the office. It is especially important to protect every area where you make contact with a debtor.

Equipment:

- Daily inspections of trucks/equipment should be conducted to ensure safe operating conditions and that equipment is operable.
- Create a checklist for those items that need to be inspected daily, weekly or monthly.
- Ensure each tow truck has the proper equipment to tow the vehicle safely (tow lights, tow straps, dollies, etc.).
- Ensure each truck/equipment has a GPS unit installed. In the event you cannot reach the driver, the vehicle can be tracked with GPS.
- Ensure each truck/equipment has a digital camera with recording capability in the event there is an issue in the field that needs documentation (accident, blocked-in vehicle, damage to residence, etc.).

Keys:

- Keys must be secured in a designated secondary locking method (lockbox, locked file cabinet or locked office accessible only to employees).
- You must have a process for securing keys after hours – for example, storing in a lockbox near the building but out of sight.
- Keys for units are never to be left in the stored vehicles at any time.

Office:

At no time should debtors or debtor representatives be allowed inside the office.

- Only visitors who have legitimate business appointments and have been prescreened should be allowed inside the office.
- All sensitive information and NPPI must be out of sight to visitors and other individuals who have no authority to view such information.
- When debtors or debtor representatives come to the office to redeem personal property or vehicles, there should be at least two staff employees in the office to witness signatures and the demeanor of the debtor or debtor's representative.
- Upon completion of the business at hand, all written documentation shall be filed in debtor's file and secured in the applicable, designated secured area.

Forms:

The forms provided in this Operations Manual are to be used as applicable to this manual. It is most important that these forms be executed and signed at the appropriate time, and that they be placed in the employee's personnel file and kept in a secured area. The supervisor who conducts the pre-employment screening must have the applicant execute the Pre-Employment Screening Form before conducting the pre-employment process.

1. **Pre-Employment Screening (Form A):** To be executed at the time an applicant for employment is interviewed.

2. **Confidentiality Agreement (Form B):** To be executed by the applicant at the time of employment. This form should be signed by any employee who did not execute it at the time of his/her hiring.

3. **Recovery Agent Code of Conduct (Form C):** To be executed by the applicant at the time of employment. This form should also be signed by any employee who did not execute it at the time of his/her hiring.

4. **Acknowledgement of Completion of Certification (Form D):** To be executed by the employee who has completed a nationally recognized and accepted certification program and can provide proof of a Certification of Completion

5. **Collateral Recovery Bankruptcy Policy (Form E):** To be executed by the employee upon review of the company's Bankruptcy Policy. If the employee has completed a certification program that meets the company's Bankruptcy Policy, his/her signature on this form will so acknowledge.

6. **Confidentiality Agreement-Vendor (Form F):** This Form must be executed by all vendors having a relationship with the company. The company owner shall be responsible for the execution of this form.

7. **CFPB Complaint Handling (Form G):** This comprehensive form outlines the information needed to process complaints in accordance with Consumer Financial Protection Bureau (CFPB) requirements.

Pre-Employment Screening (Form A)

I _____, do hereby consent to a pre-employment investigation by (Company) as one of the requirements for hiring by (Company). I further understand and agree that such pre-employment screening shall be conducted in accordance with the Fair Credit Reporting Act (FCRA), the Americans with Disabilities Act (ADA) and the Equal Employment Opportunity Commission (EEOC).

I further understand that the following types of information screened by (Company) shall include, but may not be limited to:

1. Criminal history and/or other history related to behavior that may be grounds for (Company) to deny employment. Such history includes, but is not limited to, drug or alcohol addiction, dishonesty or a propensity for violence or crimes against persons.
2. Education and other professional licensing or degrees
3. Credit history
4. History of civil violations
5. Personal references
6. Motor vehicle records

I further understand that the information screened shall be used by (Company) to determine employment or nonemployment, and that significant weight will be given to a criminal record if it includes convictions for any crime against a person, including, but not limited to, assault, battery, sex offenses and pedophilia.

Print Name _____

Signature _____ Date _____

Confidentiality Agreement; Employee (Form B)

AND NOW, on _____, this Agreement between Associated Investigators of Tampa, Inc. , a corporation, with its principal place of business at 7402 N 56th St #795, Tampa, FL 33617, hereinafter referred to as "Company" and _____, an employee of the Company, hereinafter referred to as "Employee."

WHEREAS, the Employee wishes to commence an employment relationship with the Company and the Company wishes to commence an employment relationship with the Employee and;

WHEREAS, the Employee knows that signing this Agreement is a condition of entering into an employment relationship in any manner whatsoever with the Company and the Employee fully

understands that the Employee is not being forced in any fashion whatsoever to sign this Agreement the Employee agrees to the following requirements of this Agreement;

Privacy and Data Protection. Employee agrees to comply with all privacy and data protection laws, rules and regulations as applicable now and in the future. Employee understands that he/she may come into possession of certain nonpublic personal information (NPPI) regarding or pertaining to the Company's Client customers as disclosed by Client or otherwise obtained by Employee in the performance of Employee's duties under this Agreement. Without limiting the generality of the preceding sentence, Employee agrees that they will not use or disclose to any other party any nonpublic personal information so received or obtained except as permitted by applicable law. For purposes of this Agreement, the terms "nonpublic personal information" shall have the meanings as set forth in Section 509 of the Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. Section 6809 and the implementing regulations thereof. The provisions contained in this Agreement shall survive the termination of the expiration of this Agreement, by the expiration of time, by the operation of law, or otherwise.

Information Security. Employee and Company represents and warrants to Client that they presently maintain, and will continue to maintain and periodically test the efficacy and efficiency of appropriate security programs and measures designed to ensure the security and confidentially of "Customer Information" as defined in 16 CFR 314.2(b). Such information security programs and measures shall include appropriate procedures designed to (1) protect the security and confidentiality of such information, (2) protect against anticipated threats or hazards to the security or integrity of such information, and (3) protect against unauthorized access to, or use of such information that could result in substantial harm or inconvenience to any customer of Client.

Monitoring. Due to the delicate nature of the collateral recovery industry all calls and electronic communications are subject to monitoring and recording at any time. This shall apply to and include cell phones, computers, instant messaging, telephone calls, and conversations.

Employee: _____

Signature _____ Date _____

Recovery Agent Code of Conduct (Form C)

In addition with complying with all applicable federal, state and local laws (for example, laws relating to breaching the peace), the recovery agent identified below represents and agrees that he will conduct his recovery activities in a manner consistent with the following Code of Conduct.

The repossession agent will not use any false, deceptive or misleading representations or practices, whether verbal or written, in connection with the repossession of any collateral. Without limiting this general rule, examples include:

1. Claims that the agent is affiliated with, or acting on behalf of any federal, state or local government or law enforcement agency or use any communication that would imply such an affiliation.

2. Falsely stating or implying that any individual is an attorney or that any communication is from an attorney.
3. Falsely stating the character, amount or legal status of any debt.
4. Threats to take action which cannot legally be taken, that is not intended to be taken, or that has not been authorized by “COMPANY NAME HERE” and our client.
5. Falsely stating or implying that the debtor committed any crime or other conduct.
6. Reporting or threatening to report false information to a credit reporting agency or any other person.
7. The use of any false statement or deceptive means to repossess or attempt to repossess any motor vehicle or to obtain information concerning a debtor.
8. The use of any business, company or organization name other than your own company name.
9. Falsely representing or implying that the repossession vendor is employed or affiliated with a consumer reporting agency.

The repossession agent will not engage in any conduct or practices which harass, oppress or abuse any person (not just the debtor) in connection with the repossession of a motor vehicle. Without limiting this general rule, examples include:

1. The use of or threat to use violence or other criminal means to harm the physical person, reputation or property of any person.
2. The use of obscene, profane, or abusive language.
3. The advertisement for sale of any debt to coerce payment of the debt or turnover of collateral.
4. Making telephone calls without meaningful disclosure of the caller’s identity.
5. Causing a telephone to ring or engaging any person in telephone conversation repeatedly or continuously with the intent to annoy, abuse or harass any person at the call number (e.g., a recovery agent calling and hanging up on the debtor after the debtor has hung up on them). It is not permissible to tell a debtor that you will call him/her every day until collateral is surrendered. This action would constitute harassment.
6. If at any time you perceive a customer confrontation will escalate into violence you are to immediately walk away from the scene.
7. Physical contact is NEVER acceptable.

_____ _____

Recovery Agent - Sign and Print Name Date

Acknowledgement of Completion of Nationally Accepted Certification Program (Form D)

I, _____ have completed and have been

certified through (name of program),_____ , a nationally recognized and accepted collateral recovery certification program that addresses all aspects of the self-help repossession process. Further, I have also completed the final written examination of that program and have

been issued a Certificate of Completion of that program. The certification program included the following subjects:

A. Fair Debt Collection Practices Act (FDCPA)
B. Gramm-Leach-Bliley Act (GLBA)
C. Telephone Records and Privacy Protection Act (TRPPA) HR4709
D. Service members Civil Relief Act (SCRA)
E. Uniform Commercial Code (UCC)
F. Breach of the Peace
G. Defensive Driving
H. Ethics, Professional Conduct and Communication
I. Crimes Against Persons and Property
J. The Collateral Recovery Process

Signed:_____ Date:_____

Print Name:_____

Collateral Recovery Bankruptcy Policy (Form E)

Upon notification by the customer/debtor that he/she has filed Bankruptcy, **all attempts to recover the defaulted collateral must cease**. An attempt then should be made to obtain the following information from the customer/debtor.

1. Bankruptcy case number
2. The date the bankruptcy was filed
3. Location of bankruptcy court where case was filed

4. Name and telephone number of attorney handling the bankruptcy
5. Request to see a copy of the bankruptcy filing
6. Immediately provide this information to client
7. **Await further instructions from client**

Regardless of whether the customer/debtor can, or will, provide all or part of this information, the collateral recovery specialist must cease attempts to take possession of the defaulted collateral until the information is verified as accurate and correct, and the client approves moving forward with the recovery of the defaulted collateral.

If the debtor cannot verify any of the requested information and agrees to voluntarily relinquish possession of the defaulted collateral, and the collateral recovery specialist has a viable witness that the customer/debtor voluntarily relinquished possession, the collateral recovery specialist may then secure possession. In lieu of a viable witness on scene, the collateral recovery specialist should complete a Voluntary Surrender Form and have the customer/debtor sign before securing possession.

If the collateral recovery specialist takes possession of the defaulted collateral and it is later confirmed that the Bankruptcy was in fact filed, the defaulted collateral must be returned immediately, with the customer/debtor signing a **Vehicle Redemption Form.** If the customer/debtor refuses to sign the **Vehicle Redemption Form**, the defaulted collateral is not to be released without express, written authorization from the client. It is important that the customer/debtor sign this form so that any subsequent claim by the customer/debtor that the defaulted collateral was damaged after possession was secured can be disputed.

_____Date _____

Sign and Print Name Acknowledging Policy

Confidentiality Agreement; Vendor Form (F)

Company _____, hereinafter referred to

as "Vendor," in order to continue a business relationship with;

Associated Investigators of Tampa, Inc. , or any of its affiliates, agrees to the following terms:

Vendor acknowledges that in the performance of its duties and obligations on behalf of Associated Investigators of Tampa, Inc. , that its employees, agents, assigns and/or contractors may be exposed to information relating to Associated Investigators of Tampa, Inc. , or its client's

operations, methods of doing business, research and development, clients, clients information, trade secrets, computer programs, finances, nonpublic personal information, other sensitive information, and/or other confidential and proprietary information belonging to, or in the possession of Associated Investigators of Tampa, Inc. , or any of its client's in any format whatsoever, all of which are hereinafter collectively called or referred to as "Confidential Information." Vendor agrees that it will not, nor will any of its employees, agents, assigns, and/or contractors, without express, written authorization of Associated Investigators of Tampa, Inc. acquire, use or copy, in whole or in part, the Confidential Information; Vendor further agrees that it will not, nor any of its employees, agents, assigns and/or contractors disclose, provide or otherwise make available, in whole or in part, the Confidential Information to any other person or entity of any kind whatsoever.

Vendor further agrees that it shall take all appropriate action, whether by instruction, agreement or otherwise, to ensure the protection, confidentiality and security of the Confidential Information and to satisfy its obligations with respect to this Confidentiality Agreement. Vendor further agrees that its obligations with respect to the confidentiality and security of the Confidential Information exposed to the Vendor, its employees, agents, assigns and/or contractors, shall survive the termination of any agreement or relationship between Associated Investigators of Tampa, Inc. and Vendor. Vendor further agrees that this Agreement shall be governed by the laws of the State of Florida and acknowledges that it has received a copy of the Confidentiality Agreement as executed by Vendor's authorized representative.

(Vendor Name)_____

Type of service provided _____

Authorized representative _____

Signature _____Date, _____

Title _____

CFPB Complaint Handling Checklist (Form G)

Complaint Handling Checklist

	Yes	No
Company has policy of complaint handling	**X**	☐
Policy is documented	**X**	☐
Policy is available to staff and customers	**X**	☐

Policy is reviewed annually	X	☐
Policy is written in plain, understandable English	X	☐

Company complaint process has the following features:

Open and accessible to the public	X	☐
Clearly understood procedure for people to make complaints	X	☐
A statement of who is responsible for dealing with complaints	X	☐
Procedure for resolving, investigating and handling complaints depending on their seriousness and complexity	X	☐
Clearly understood procedure for people to make suggestions for improvement	X	☐
A system for keeping the complainant informed of the complaint process	X	☐
A system for recording complaints and outcomes	X	☐
Procedures for protecting the confidentiality of complaint details	X	☐
A system of feedback to relevant areas of management and operations so that the problem and trends identified from complaint can be incorporated into planning activities	X	☐
Effective complaint handling is supported by senior management	X	☐
Senior management is responsible for effective operation of the complaint system	X	☐

Policy and procedures associated with the complaint

system are communicated to the staff	X	☐
Adequate resources are allocated to enable complaint system to function	X	☐
Complaint handling responsibilities are incorporated into staff position descriptions	X	☐
Staff have specific instructions on how to handle complaints	X	☐
Staff is given written instructions on complaint procedures	X	☐
There is a comprehensive complaint handling instructions manual for staff	X	☐
The complaint manual is regularly reviewed and updated	X	☐
The complaint procedures manual is easily accessible to any staff member	X	☐
The procedures or complaint manual provides guidance on what remedies can or should be used to resolve complaints	X	☐
Customers are told how to make a complaint	X	☐
Complaint forms are readily available to customers	X	☐
Complaint forms or signs are displayed prominently in public areas and are readily accessible	X	☐
Complaint information is included on company's website	X	☐

Customers are able to lodge complaints:

in writing	X	☐
by email	X	☐
by fax	X	☐
by telephone	X	☐

in person	X	☐
via company's website	☐	X
Customers are provided assistance to make complaints where needed	X	☐
Complaint system is free of charge	X	☐
Complaints are recorded in a complaint database	X	☐
Outcomes of complaints are recorded	X	☐
There are performance standards in place for the way in which complaints are dealt with:	X	☐
Acknowledgment of receipt within a certain time	X	☐
Completion/resolution within a certain time	X	☐
There is a quality control system in place to:		
Check if all complaints have been dealt with	X	☐
Check if all aspects of complaints have been addressed	X	☐
Check if all necessary follow-up action has been taken	X	☐
Check if the underlying problem has been identified and addressed	X	☐