EAGLE GROUP XX

SUPPORT EMPLOYEE COMPLIANCE TRAINING

"SECT"

DISCLAIMER

This information is not intended to be legal advice and may not be used as legal advice. Legal advice must be tailored to the specific circumstances of each case.

Every effort has been made to assure this information is up-to-date. It is not intended to be a full and exhaustive explanation of the law in any area, however, nor should it be used to replace the advice of your own legal counsel.

The views and opinions expressed herein are solely those of the members of EAGLE GROUP XX. The information and any materials provided "as is" and the members of EAGLE GROUP XX expressly disclaim all warranties, conditions, representations, indemnities and guarantees whether express or implied, arising by law or custom.

In no event will the members of EAGLE GROUP XX be held liable for any claim or action arising from or related to your failure to comply with any laws or regulations.

Your use of the materials constitutes full and sufficient consideration for, and acceptance by you, of the above terms.

The purpose of the Support Employee Compliance Training "SECT" is to develop a uniform training program the purpose of which is to educate and train the personnel who work in the recovery agency office and who in the course of their duties, come into contact with consumers and third parties.

This program was developed by Eagle Group XX member agencies with two primary goals in mind, one, to insure that their support employees were properly trained to perform their duties in a compliant, safe and legal manner and two, to insure that the consumers and third parties the employees came into contact with were treated professionally, fairly, and the consumer's privacy rights were protected.

CONTENTS

I. PROTECTING NON-PUBLIC PERSONAL INFORMATION (NPPI)

One of the primary responsibilities of support personnel at an asset recovery agency is the protection of consumer data. This section deals with the areas of data movement through and agency and the precautions which must be observed.

Effective data security starts with assessing what information you have and identifying who has access to it. Understanding how personal information moves into, through and out of your business and who has, or could have, access to it is essential to assessing security vulnerabilities. You can determine the best ways to secure the information only after you've traced how it flows.

Inventory all computers, laptops, flash drives, disks, home computer, and other equipment to find out where your company stores sensitive data. Also inventory the information you have by type and location. Your file cabinets and computer systems are a start, but remember, your business receives personal information in a number of ways – through websites, from contractors, from call centers, and the like. What about information saved on laptops, employees' home computers, flash drives, and cell phones? No inventory is complete until you check everywhere sensitive data might be stored.

Track personal information through your business by taking with your sales department, information technology staff, human resources office, accounting personnel, and outside service providers. Get a complete picture of:

Who sends sensitive personal information to your business?

- Do you get it from Lenders? Banks or other financial institutions? Credit bureaus? Data Providers? Other businesses?
- *How does your business receive personal information?*
- Does it come to your business through a website? By email? Through the mail? Is it transmitted through industry gateways?
- *What kind of information you collect at each entry point?* Do you get credit data information online? Does your agency keep information about consumers?

Where do you keep the data you collect at each entry point?

- Is it in a central computer database? On individual laptops? On disks or lap-tops? In file cabinets? Do employees have files in their personal possession? How is the data protected in transit and at rest?
- *Who has* – or could have – access to the information?
- Which of your employees has permission to access the information? Could anyone else get a hold of it? What about vendors who supply and update software. Vendors who have access to your office and/or secured areas where data is stored? Contractors?
- Different types of information present varying risks. Pay attention to how you keep personally identifying information: Social Security numbers, credit card or financial information, and other sensitive data. That's what thieves use most often to commit fraud or identity theft, If possible review the assignment to ensure all the required documents are present including a copy of the title or a UCC 1 filing document or the vehicle title clearly identifying the lien holder as being your client and insuring that they have a valid security interest in the vehicle identified on your assignment.
- If possible, review the client's notes if available and make a special note of any unusual circumstances.
- If possible, verify the documents supplied by the client contain the current balance, date of last pay, amount past due and the last known verified location of the collateral.
- If required information is not present it is recommended the client be contacted and the information be obtained prior to working the assignment.

PHYSICAL SECURITY OF DATA

The degree and frequency of data protection inspections must be set by the compliance officer at each agency and depending on size, number of employees and exposure risks will vary from agency to agency. Issues that must be addressed include but are not limited to:

- Computer Screens/Black Screen-Clean Desk Policy
- Camera Recording Equipment
- Safety Equipment

- All Storage Containers
- Employee and non-employee access
- Agency Data Privacy Policies ○ GLBA ○ TRPPA ○ FDCPA
  ○ HIPAA

II. COMPLIANCE POLICIES

These are Security and Privacy policies that each agency should have to comply with statutes. Each state may also have Security and Privacy statutes related to protection of NPPI data.

- Assignment of Access Privileges Policy
- Minimum Necessary Rule
- NPPI Security P&P Checklist
- System Security
- Written Information Security Plan (WISP)
- Red Flag Identification Policy
- Document Retention-Protection-Destruction Policy
- Data Breach Notification Letter Policy
- Fraud Identification Theft Client Notification Form
- Consumer Dispute Notification Form
- Notification of Findings
- Clean Desk Policy
- Clean Desk & Clear Screen Policy
- Clean Desk & Clear Screen Log
- Critical Vendor Assessment Form
- Hand-Held Communication Instrument Policy

CONSUMER COMPLAINT RESPONSE & TRACKING POLICY

These are Complaint Response and Tracking policies that each agency should have to comply with statutes. Each state may also have Consumer Complaint Response and Tracking statutes.

- Complaint Response Guidelines
- Complaint Response Process

- Consumer Dispute Form Log
- Ownership Responsibility
- Application
- Control Objective
- Acknowledgement Letter
- Consumer Dispute Form Policy
- Consumer Dispute Form
- Consumer Dispute Supervisor Form
- Consumer Dispute Property Damage Form Affidavit of Facts
- Third Party Disagreement/Problem Report
- Categorizing and Response to Disputes
- UDAAP Policy & Procedures
- Anti-Bullying Policy
- Anti-Discrimination & Harassment Policy
- Limited English Proficiency Policy
- Anti-Money Laundering Policy
- No Weapons Policy
- Skip Tracing & Asset Searching Policy
- Communication Policy

III. POST RECOVERY CONTACT WITH CONSUMERS

Repossession, the act of recovering mortgaged property covered by a defaulted security agreement, is one of the most invasive processes of the credit/collection process and requires a complete understanding of the actions involved to make sure that the recovery is performed in a safe, compliant and legal manner.

There are certain compliance policies and procedures that should be followed by support personnel to increase the probability of a safe and compliant post recovery encounter with a consumer which will result in a pleasant professional experience rather than an angry and dangerous confrontation.

When working in the agency office where a support person may have direct contact with a consumer the employee's appearance becomes a very important issue. A support person should present a business-like appearance and demeanor therefore each agency should have a written dress code for all employees and the code should be monitored and enforced on a regular basis.

Training in Conditions: WHITE – ORANGE – RED – BLACK

WHITE

Unaware of surroundings or possible threats. (listening to music, conversing with fellow employees, reading, etc.)

ORANGE

Aware of surroundings or possible threats, paying attention to what is going on at that particular moment and prepared to react accordingly. (Consumer has become loud and threatening, placing hands in pocket for a possible weapon, body language indicates physical threat.)

RED

Threat or incident has occurred requiring action on the part of the employee. (Summoning assistance, phoning law enforcement, seeking physical protection.)

BLACK

Injury or death has occurred.

When Contacted by a Consumer:

- Remain calm, speak and behave in a professional manner.
- Identify yourself to the consumer as any person or thing other than whom and what you are.
- Identify yourself as an employee of the recovery agency.
- Do not discuss the debt or divulge any information regarding the case to any party other than the consumer, spouse or co-maker on the debt.
- Talk down, threaten or attempt to intimidate any person.
- Verbally abuse or physically touch anyone.
- If the consumer becomes abusive or threatening request the aid of law enforcement personnel for assistance.

CONFRONTATIONAL AVOIDANCE TECHNIQUES

Occasionally a support employee must deal with anger in the people they come into contact with. It is imperative that the agent maintain control of the situation and avoid any actions which could lead to violence. These few basic mitigation techniques, used by professional

asset recovery specialists, should be recognized, mastered in order that they might be utilized when needed.

FOGGING – ECHOING – DISARMING – ISOLATING - STEPPING

FOGGING...

- Disarm your adversary by agreeing with them whenever possible with whatever truth, generalization or probability they present. Always remember that in all possibility there is some truth, even though greatly exaggerated in what they are being said.

ECHOING...

- Echoing what your adversary says lets them know that you not intend to argue or fight over differences. Always remember that it takes two to argue, and if you refuse to participate in the conflict, you will have a greater control over the situation.

DISARMING...

- Always give your adversary the opportunity to reconsider and retract any rash or threatening statement. You may accomplish this maneuver by saying, "Excuse me, I don't think I quite understand what you just said." An adversary will usually not repeat their statements and it allows for a pause in the conversation which may cool things off.

ISOLATING...

- You may be able to calm a potentially volatile situation down by talking to your adversary in private. Many times when deprived of an audience a person will change their attitude and problems can be resolved much easier.

STEPPING...

- In many instances stepping out of the ring is the only way to calm an adversary down. This tactic lets your adversary know they have possibly gone too far. A good statement to use is, "I am finding it very difficult to communicate with you right now and if we are unable to communicate, we certainly cannot resolve this problem. Maybe you need to deal with someone else or discuss it at another time. Get out of the ring and there can be no fight.

IV. ADDITIONAL RESPONSIBILITIES

PROTECTION OF PERSONAL PROPERTY

Responsibility for safekeeping of personal property must be a primary concern for the recovery agency and the support employees; therefore policy must be established and followed to make sure that a consumer's property is properly protected from the time the agent takes possession of the collateral until the consumer claims the property.

It is recommended that a witness be present when vehicle contents are inventoried and that all employees conducting inventory of personal property protect themselves by wearing protective gloves, clothing and in many cases breathing masks.

- ❑ A primary tool for safekeeping personal property and maintaining a proper chain of control is the "Personal Property Inventory". This document should be completed as soon as possible after securing a vehicle and witnessed by at least one person other than the agent. The document should be filled out in detail showing the complete contents including the glove box, center console and trunk where applicable and accessible. It should be noted if any storage areas are locked and if there is no personal property in the vehicle, even in cases of a voluntary surrender, the same should be noted on the "Personal Property Inventory" sheet.
- ❑ In cases where contraband items such as drugs, firearms, explosives, etc. are found the items should be noted and turned over to local law enforcement agencies with the condition report clearly indicated the time, date and agency retrieving the property.
- ❑ In many cases agent conducting inventory of personal property will find HIPPA protected property. This property is easily defined as "any item or document which is in any way medically related". This property should be kept in a separate container and properly sealed to protect the consumer's medical privacy.

Continue to Exam

SUPPORT EMPLOYEE COMPLIANCE TRAINING (SECT) Exam V1