ACTION RECOVERY & COLLECTIONS

425 SHAMBURGER LN.
LITTLE ROCK, AR. 72206

FRAUD DETECTION and IDENTITY THEFT PROGRAM

2009-2010

Date___/___/____

INTRODUCTION

Recognizing that Identity Theft is the number one white collar crime in America today and in compliance with recent rulings of the Federal Trade Commission, Action Recovery & Collections LLC has established and implemented programs to prevent fraud and identity theft.

This program covers the requirements of the FTC and was designed with the aid and guidelines as presented in the FTC Guide, "Protecting Personal Information, A Guide for Business". Each step recommended in the guide was discussed by our management and compliance personnel and, where required, programs established and implemented. The Guide itself then became part of our basic program related to fraud and identity protections.

The Action Recovery & Collections LLC Compliance officers were required to attend the Time Finance Adjustors Seminar, "The Credit and Collection Officer Compliance Workshop" prior to setting up the necessary security program to protect consumer data given to Action Recovery & Collections LLC by clients as well as other programs related to data protection and security.

These Action Recovery & Collections LLC Compliance officers will continue to monitor the fraud and identity theft policies and procedure and update as is necessary.

Included in this package are the documents used pursuant to FDCPA, FCRA/FACTA, HIPPA, TCPA, TRPPA, GLBA and the "RED FLAG RULES" to ensure compliance. These documents are proprietary to Action Recovery & Collections LLC and any unauthorized use or distribution is strictly prohibited.

TABLE OF CONTENTS

Protecting
PERSONAL INFORMATION
A Guide for Business

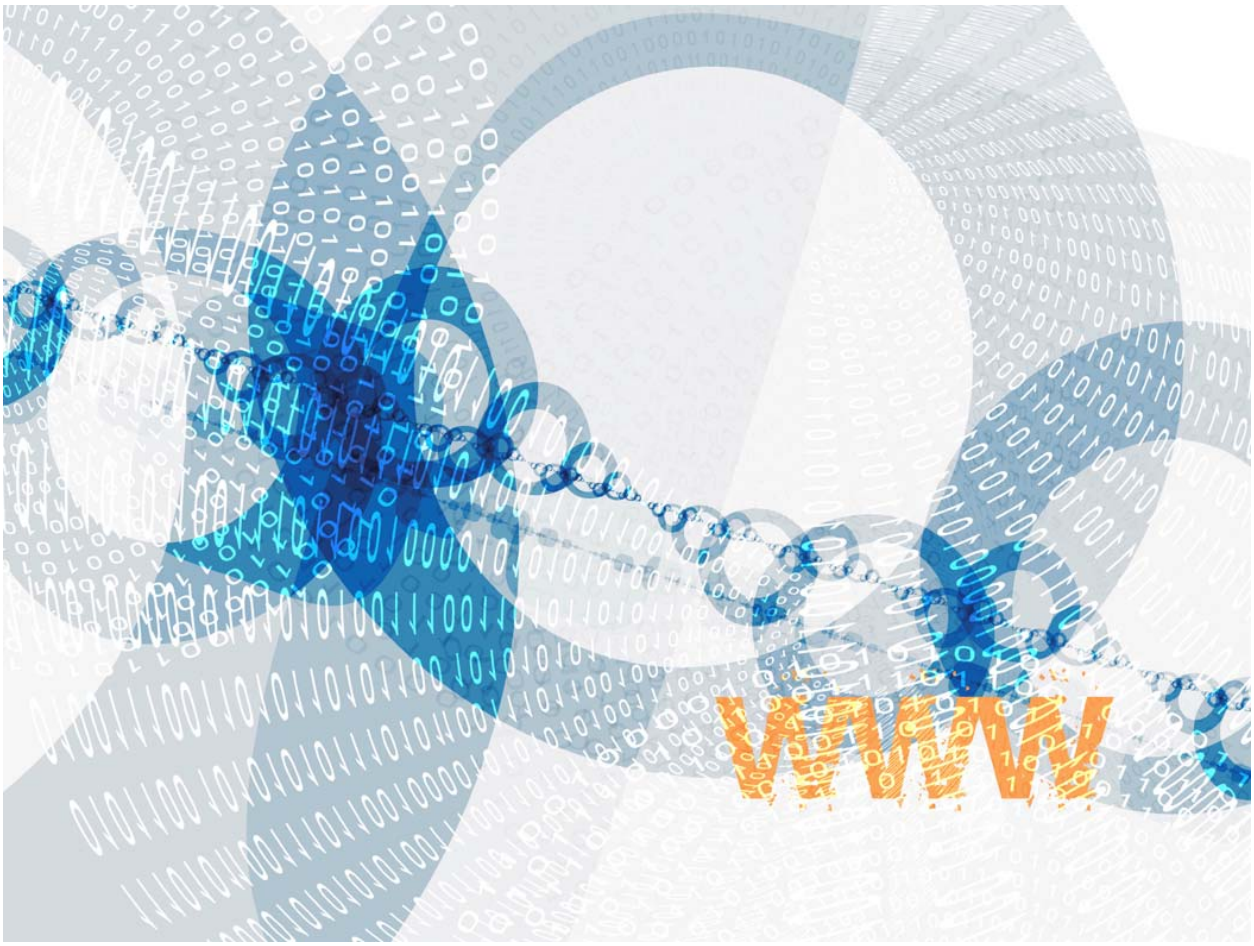
FEDERAL TRADE COMMISSION

PROTECTING PERSONAL INFORMATION
A Guide for Business

Most companies keep sensitive personal information in their files-----names, Social Security numbers, credit card, or other account data-----that identifies customers or employees.

This information often is necessary to fill orders, meet payroll, or perform other necessary business functions. However, if sensitive data falls into the wrong hands, it can lead to fraud, identity theft, or similar harms. Given the cost of a security breach-----losing your customers' trust and perhaps even defending yourself against a lawsuit-----safeguarding personal information is just plain good business.

Some businesses may have the expertise in-house to implement an appropriate plan. Others may find it helpful to hire a contractor. Regardless of the size-----or nature-----of your business, the principles in this brochure will go a long way toward helping you keep data secure.



FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-FTC-HELP (1-877-382-4357)
ftc.gov/infosecurity

A sound data security plan is built on 5 key principles:

1. **Take stock.** Know what personal information you have in your files and on your computers.

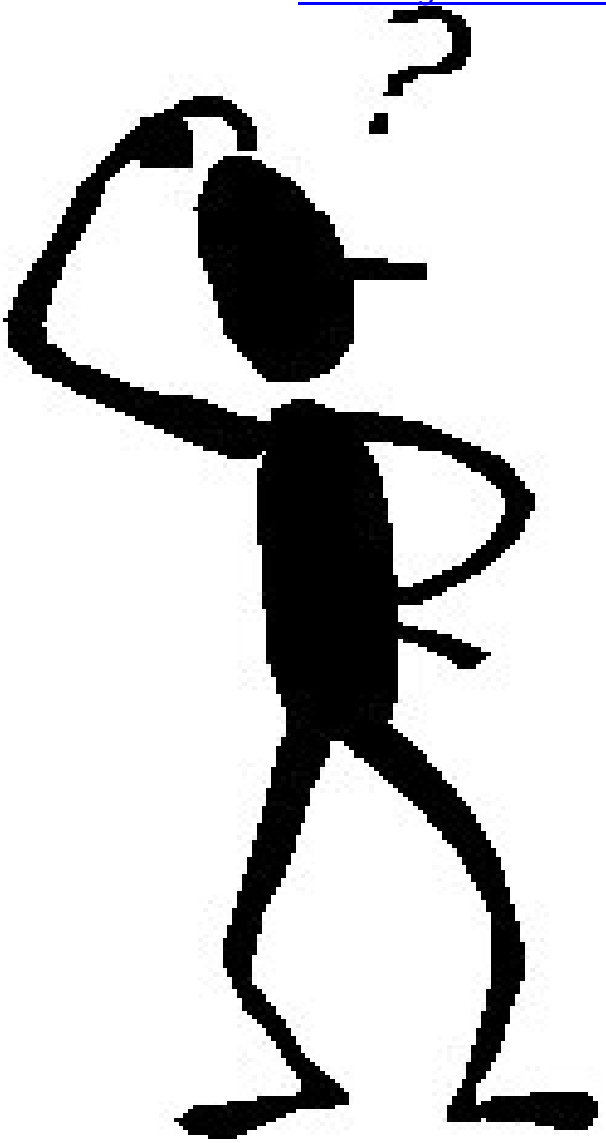
2. **Scale down.** Keep only what you need for your business.

3. **Lock it.** Protect the information that you keep.

4. **Pitch it.** Properly dispose of what you no longer need.

5. **Plan ahead.** Create a plan to respond to security incidents.

Use the checklists on the following pages to see how your company's practices measure up---and where changes are necessary. You also can take an interactive tutorial at *www.ftc.gov/infosecurity*.



1. TAKE STOCK. Know what personal information you have in you files and on you computers.

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 files 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 customers? Credit card companies? Banks or other financial institutions? Credit bureaus? Other businesses?

  - ***How your business receives personal information.*** Does it come to your business through a website? By email? Through the mail? Is it Transmitted through cash registers in stores?

  - ***What kind of information you collect at each entry point.*** Do you get credit card information online? Does your accounting department keep information about customers' checking accounts?

  - ***Where you keep the information you collect at each entry point.*** Is it in a central computer database? On individual laptops? On disks or tapes? In file cabinets? In branch offices? Do employees have files at home?

✓ **SECURITY CHECK**

Question:
Are there laws that require my company to keep sensitive data secure?

Answer:
Yes. While you're taking stock of the Data in your files, take stock of the law, too statutes like the Gramm-Leach-Bliley Act, the Fair Credit Reporting act, and the Federal Trade Commission Act may require you to provide reasonable security for sensitive information.

To find out more, visit www.ftcgov/privacy.

- ❖ ***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 you use to process credit card transactions? Contractors operating your call center?

- Different types of information present varying risks. Pay particular 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.

2. SCALE DOWN. Keep only what you need for your business.

If you don't have a legitimate business need for sensitive personally identifying information, don't keep it. In fact, don't even collect it. If you have a legitimate business need for the information, keep it only as long as it's necessary.

- Use Social Security numbers only for required and lawful purposes — like reporting employee taxes. Don't use Social Security numbers unnecessarily — for example, as an employee or customer identification number, or because you've always done it.

> ✓ **SECURITY CHECK**
>
> **Question:**
> We like to have accurate information about our customers, so we usually create a permanent file about all aspects of their transactions, including the information we collect from the magnetic stripe on their credit cards. Could this put their information at risk.
>
> **Answer:**
> Yes. Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it if it's not in your system, it can't be stolen by hackers.

- The law requires you to shorten — or truncate — the electronically printed credit and debit card receipts you give your customers. You may include no more than the last five digits of the card number, and you must delete the expiration date.

- Don't keep customer credit card information unless you have a business need for it. For example, don't retain the account number and expiration date unless you have an essential business need to do so. Keeping this information — or keeping it longer than necessary — raises the risk that the information could be used to commit fraud or identity theft.

- Check the default setting on your software that reads customers' credit card numbers and processes the transactions. Sometimes it's preset to keep information permanently. Change the default setting to make sure you're not keeping information you don't need.

- If you must keep information for business reasons or to comply with the law, develop a written records retention policy to identify what information must

- be kept, how to secure it, how long to keep it and how to dispose of it securely when you no longer need it.

3. **LOCK IT.** Protect the information that you keep.

What's the best way to protect the sensitive personally identifying information you need to keep? It depends on the kind of information and how it's stored. The most effective data security plans deal with four key elements: physical security, electronic security, employee training, and the security practices of contractors and service providers.

PHYSICAL SECURITY
Many data compromises happen the old-fashioned way — through lost or stolen paper documents. Often, the best defense is a locked door or an alert employee.

- Store paper documents or files, as well as CDs, floppy disks, zip drives, tapes and backups containing personally identifiable information in a locked room or in a locked file cabinet. Limit access to employees with a legitimate business need. Control who has a key, and the number of keys.

- Require that files containing personally identifiable information be kept in locked file cabinets except when an employee is working on the file. Remind employees not to leave sensitive papers out on their desks when they are away from their workstations.

- Require employees to put files away, log off their computers, and lock their file cabinets and office doors at the end of the day.

- Implement appropriate access controls for your building. Tell employees what to do and whom to call if they see an unfamiliar person on the premises.

- If you maintain offsite storage facilities, limit employee access to those with a legitimate business need. Know if and when someone accesses the storage site.

- If you ship sensitive information using outside carriers or contractors, encrypt the information and keep an inventory of the information being shipped. Also use an overnight shipping service that will allow you to track the delivery of your information.

ELECTRONIC SECURITY

Computer security isn't just the realm of your IT staff. Make it your business to understand the vulnerabilities of your computer system, and follow the advice of experts in the fields.

General Network Security

- Identify the computers or servers where sensitive personal information is stored.

- Identify all connections to the computers where you store sensitive information. These may include the Internet, electronic cash registers, computers at your branch offices, computers used by service providers to support your network, and wireless devices like inventory scanners or cell phones.

- Assess the vulnerability of each connection to commonly known or reasonable foreseeable attacks. Depending on your circumstances, appropriate assessments may range from having knowledgeable employee run off-the-shelf security software to having an independent professional conduct a full-scale security audit.

- Don't store sensitive consumer data on any computer with an Internet connection unless it's essential for conducting your business.

- Encrypt sensitive information that you send to third parties over public networks (like the Internet), and consider encrypting sensitive information that is stored on your computer network or on disks or portable storage deices used by your employees. Consider also encrypting email transmissions within your business if they contain personally identifying information.

- Regularly run up-to-date anti-virus and anti-spyware programs on individual computers and on servers on your network.

- Check expert websites (such as www.sans.org) and your software vendors' websites regularly for alerts about new vulnerabilities, and implement policies for installing vendor-approved patches to correct problems.

- Scan computers on your network to identify and profile the operating system and open network services. If you find services that you don't need, disable then to prevent hacks or other potential security problems. For example, if email service or an Internet connection is not necessary on a certain computer, consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

✓ **SECURITY CHECK**

Question:
We encrypt financial data customers submit on our website. But once we receive it, we decrypt it and email it over the intranet to our branch offices in regular text is there a safer practice?

Answer:
Yes. Regular email is not secure method for sending sensitive data. The better practice is to encrypt any transmission that contains information that could be used by fraudsters or ID thieves.

- When you receive or transmit credit card information or other sensitive financial data, use Secure Sockets Layer (SSL) or another secure connection that protects the information in transit.

- Pay particular attention to the security of your web application — the software used to give information to visitors to your website and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks. In one variation called an "injection attack", a hacker inserts malicious commands into what looks like a legitimate request for information. Once in your system, hackers transfer sensitive information from your network to their computers. Relatively simple defenses against these attacks are available form a variety of sources.

Password Management

- Control access to sensitive information by requiring that employees use “strong” Passwords. Tech security experts say the longer the password, the better. Because simple passwords — like common dictionary words — can be guessed easily, insist that employees choose passwords with a mix of letters, numbers, and characters. Require an employee’s user name and password to be different, and require frequent changes in passwords.

- Explain to employees why it’s against company policy to share their passwords or post them near their workstations.

- Use password-activated screen savers to lock employee computers after a period of inactivity.

- Lock out users who don’t enter the correct password within a designated number of log-on attempts.

> ✓ **SECURITY CHECK**
>
> **Question:**
> Our account staff needs access to our database of customer financial information. To make it easier to remember, we just use our company name as the password. Could that create a security problem?
>
> **Answer:**
> Yes. Hackers will first try words like “password”, your company name, the software’s default password, and other easy-to-guess choices. They’ll also use programs that run through common English words and dates To make it harder for them to crack your system, select strong password — the longer, the better — that use a combination of letters, symbols, and numbers. And change passwords often.

- Warn employees about possible calls from identity thieves attempting to deceive them into giving out their passwords by impersonating members of your IT staff. Let employees know that calls like this are always fraudulent, and that no one should be asking them to reveal their passwords.

- When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.

- Caution employees against transmitting sensitive personally identifying data — Social Security numbers, password, account information — via email. Unencrypted email is not a secure way to transmit any information.

Laptop Security

- Restrict the use of laptops to those employees who need them to perform their jobs.

- Assess whether sensitive information really needs to be stored on a laptop. If not, delete it with a “wiping” program that overwrites data on the laptop. Deleting files using standard keyboard commands isn’t sufficient because data may remain on the laptop’s hard drive. Wiping programs are available at most office supply stores.

- Require employees to store laptops in a secure place. Even when laptops are in use, consider using cords and locks to secure laptops to employees’ desks.

- Consider allowing laptop users only to access sensitive information, but not to store the information on their laptops. Under this approach, the information is stored on a secure central computer and the laptops function as terminals that display information from the central computer, but do not store it. The information could be further protected by requiring the use of a token, “smart card,” thumb print, or other biometric — as well as a password — to access the central computer.

- If a laptop contains sensitive data, encrypt it and configure it so users can’t download any software or change the security settings without approval from your IT specialists. Consider adding an “auto-destroy” function so that data on a computer that is reported stolen will be destroyed when the thief uses it to try to get on the Internet.

- Train employees to be mindful of security when they’re on the road. They should never leave a laptop visible in a car, at a hotel luggage stand, or packed in checked luggage unless directed to by airport security. If someone must leave a laptop in a car, it should be locked in a trunk. Everyone who goes through airport security should keep an eye on their laptop as it goes on the belt.

Firewalls

- Use a firewall to protect your computer from hacker attacks while it is connected to the Internet. A firewall is software or hardware designed to block hackers from accessing your computer. A properly configured firewall makes it tougher for hackers to locate your computer and get into your programs and files.

- Determine whether you should install a “border” firewall where your network connects to the Internet. A border firewall separates your network from the internet and may prevent an attacker from gaining access to a computer on the network where you store sensitive information. Set “access controls”—settings that determine who gets through the firewall and what they will be allowed to see — to allow only trusted employees with a legitimate business need to access the

network. Since the protection a firewall provides is only as effective as its access controls, review them periodically.

- If some computers on your network store sensitive information while others do not, consider using additional firewalls to protect the computers with sensitive information.

Wireless and Remote Access

- Determine if you use wireless devices like inventory scanners or cell phones to connect to your computer network or to transmit sensitive information.

- If you do, consider limiting who can use a wireless connection to access your computer network. You can make it harder for an intruder to access the network by limiting the wireless devices that can connect to your network.

- Better still; consider encryption to make it more difficult for an intruder to read the content. Encrypting transmissions from wireless devices to your computer network may prevent an intruder from gaining access through a process called “spoofing”— impersonating one of your computers to get access to your network.

- Consider using encryption if you allow remote access to your computer network by employees or by service providers, such as companies that troubleshoot and update software you use to process credit card purchases.

Detecting Breaches

- To detect network breaches when they occur, consider using an intrusion detection system. To be effective, it must be updated frequently to address new types of hacking.

- Maintain central log files of security-related information to monitor activity on your network so that you can spot an respond to attacks. If there is an attack on your network, the log will provide information that can identify the computers that have been compromised.

- Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

- Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from your system to an unknown user. If large amounts of information are being transmitted from your network, investigate to make sure the transmission is authorized.

- Have in place and implement a breach response plan.

EMPLOYEE TRAINING

Your data security plan may look great on paper, but it's only as strong as the employees who implement it. Take time to explain the rules to your staff, and train them to spot security vulnerabilities. Periodic training emphasizes the importance you place on meaningful data security practices. A well-trained workforce is the best defense against identity theft and data breaches.

- Check references or do background checks before hiring employees who will have access to sensitive data.

- Ask every new employee to sign an agreement to follow your company's confidentiality and security standards for handling sensitive data. Make sure they understand that abiding by your company's data security plan is an essential part of their duties. Regularly remind employees of your company's policy—and any legal requirement—to keep customer information secure and confidential.

- Know which employees have access to consumers' sensitive personally identifying information. Pay particular attention to data like Social Security numbers and account numbers. Limit access to personal information to employees with a "need to know"

- Have a procedure in place for making sure that workers who leave your employ or transfer to another part of the company no longer have access to sensitive information. Terminate their passwords, and collect keys and identification cards as part of the check-out routine.

✓ **SECURITY CHECK**

Question:
I'm not really a "tech" type Are there steps our computer people can take to protect our system from common hack attacks?

Answer:
Yes. There are relatively simple fixes to protect your computers from some of the most common vulnerabilities for example, a threat called an "SOL injection attack" can give fraudsters access to sensitive data on your system, but can be thieved with a simple change to your computer. Bookmark the websites of groups like the Open Web Application Security Project, www.owasp.org., SANS (SysAdmin, Audit, Network, Security) Institute's Most Critical Internet Security Vulnerabilities, www.sans.org/top20 for up-to-date information on the latest threats—and fixes. And check with your software vendors for patches that address new vulnerabilities.

- Create a “culture of security” by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities. Make sure training includes employees at satellite offices, temporary help, and seasonal workers. If employees don’t attend, consider blocking their access to the network.

- Train employees to recognize security threats. Tell them how to report suspicious activity and publicly reward employees who alert you to vulnerabilities.

- Consider asking your employees to take the FTC’s plain-language, interactive tutorial at www.ftc.gov/infosecurity.

- Tell employees about your company policies regarding keeping information secure and confidential. Post reminders in areas where sensitive information is used or stored, as well as where employees congregate. Make sure your policies cover employees who telecommute or access sensitive data from home or an off site location.

- Warn employees about phone phishing. Train them to be suspicious of unknown callers claiming to need account numbers to process an order or asking for customer or employee contact information. Make it office policy to double-check by contacting the company using a phone number you know is genuine.

- Require employees to notify you immediately if there is a potential security breach, such as a lost or stolen laptop.

- Impose disciplinary measures for security policy violations.

- For computer security tips, tutorials and quizzes for everyone on your staff, visit www.OnGuardOnline.gov.

SECURITY PRACTICES OF CONTRACTORS AND SERVICE PROVIDERS

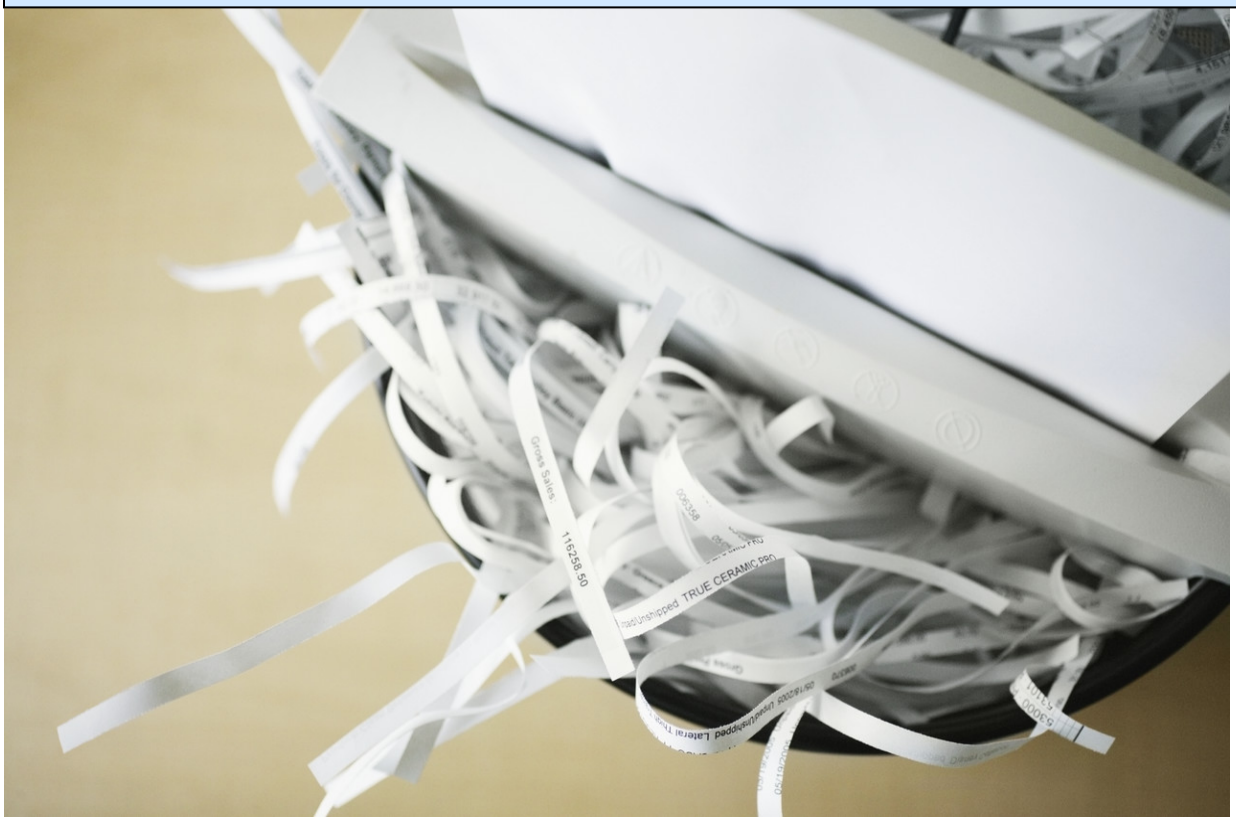
Your company’s security practices depend on the people who implement them, including contractors and service provider.

- ❖ Before you outsource any of your business functions—payroll, web hosting, customer call center operations, data processing, or the like—investigate the company’s data security practices and compare their standards to yours. If possible, visit their facilities.

- ❖ Address security issues for the type of data your service providers handle in your contract with them.

- ❖ Insist that your service providers notify you of any security incidents they experience, even if the incidents they experience, even if the incidents may not have led to an actual compromise of your data.

4. PITCH IT. Properly dispose of what you no longer need.



What looks like a sack of trash to you can be a gold mine for an identity thief. Leaving credit card receipts or papers or CD's with personally identifying information in a dumpster facilitates fraud and exposes consumers to the risk of identity theft. By properly disposing of sensitive information, you ensure that it cannot be read or reconstructed.

- Implement information disposal practices that are reasonable and appropriate to prevent unauthorized access to—or use of—personally identifying information. Reasonable measures for your operation are based on the sensitivity of the information, the costs and benefits of different disposal, methods, and changes in technology.

✓ **SECURITY CHECK**

Question:
My company collects credit applications from customers. The form requires them to give us lots of financial information. Once we're finished with the applications we're careful to throw them away. Is that sufficient?

Answer:
No. Have a policy in place to ensure that sensitive paperwork is unreadable before you throw it away. Burn it, shred it, or pulverize it to make sure identity thieves can't steal it from your trash.

- Effectively depose of paper records by shedding, burning, or pulverizing them before discarding. Make shredders available throughout the workplace, including next to the photocopier.

- When disposing of old computers and portable storage devices, use wipe utility programs. They're inexpensive and can provide better results by overwriting the entire hard drive so that the files are no longer recoverable. Deleting files using the keyboard or mouse commands usually isn't sufficient because the files may continue to exist on the computer's hard drive and could be retrieved easily.

- Make sure employees who work from home follow the same procedures for disposing of sensitive documents and old computers and portable storage devices.

- If you use consumer credit reports for a business purpose, you may be subject to the FTC's Disposal Rule. For more information, see *Disposing of Consumer Report Information? New Rule Tells How at www.ftc.gov (just enter the title into the search engine).*

5. PLAN AHEAD. Create a plan for responding to security incidents.

Taking steps to protect data in your possession can go a long way toward preventing a security breach. Nevertheless, breaches can happen. Here's how you can reduce the impact on your business, your employees, and your customers:

- Have plan in place to respond to security incidents. Designate a senior member of your staff to coordinate and implement the response plan.

- If a computer is compromised, disconnect it immediately from the Internet.

> ✓ **SECURITY CHECK**
>
> **Question:**
> I own a small business Aren't these precautions going to cost me a mint to implement?
>
> **Answer:**
> No. There's no one-size-fits all approach to data security, and what's right for you depends on the nature of your business and the kind of information you collect from your customers. Some of the most effective security measures—using strong passwords, locking up sensitive paperwork, training your staff etc.—will cost your next to nothing and you'll find free or low cost security tools at non-profit websites dedicated to data security furthermore, it's cheaper in the long run to invest in better data security that to lose the goodwill of your customers defend yourself in legal actions, and face other possible consequences of a data breach.

- Investigate security incidents immediately and take steps to close of existing vulnerabilities or threats to personal information.

- Consider whom to notify in the event of an incident, both inside and outside your organization. You may need to notify consumers, law enforcement, customers, credit bureaus, and other businesses that may be affected by the breach. In addition, many states and the federal bank regulatory agencies have laws or guidelines addressing data breaches. Consult your attorney.

ADDITIONAL RESOURCES

These websites and publications have more information on securing sensitive data:

- Federal Trade Commission's Interactive Tutorial www.ftc.govinfosecurity
- National institute of Standards and Technology (NIST)'s Computer Security Resource Center www.cstc.nist.gov
- NIST's Risk Management guide for Information Technology Systems www.csrc.nist.gov/publications/ nistpubs/800-30/sp800-30.pdf
- Department of Homeland Security's National Strategy to Secure Cyberspace www.dhs.gov/xlibrary/assets/ National_Cyberspace_Strategy.pdf
- SANS (SysAdmin, Audit, Network, Security) Institute's Most Critical Internet Security Vulnerabilities www.sans.org/top20
- United States Computer Emergency Readiness Team (US-CERT) www.us-cert.gov
- Carnegie Mellon Software Engineering Institute's CERT Coordination Center www.cert.org/orther_sources
- Center for Internet Security (CIS) www.cisecurity.org
- The Open Web Application Security Project www.owasp.org
- OnGuard Online www.OnGuardOnline.gov

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit ftc.gov or call toll-free 1-877-FTC-HELP (1-877-832-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments form small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to www.sba,gov/ombudsman.

Information Compromise and the Risk of Identity Theft:
Guidance for Your Business

These days, it is almost impossible to be in business and not collect or hold personally identifying information – names and address, Social Security numbers, credit card numbers, or other account number – about your customers, employees, business partners, student, or patients. If this information falls into the wrong hand, it could put these individual at risk for identity theft.

Still, not all personal information compromises result in identity theft, and the type of personal information compromised can significantly affect the degree of potential damage. What steps should you take and whom should you contact if personal information is compromised? Although the answers vary from case to case, the following guidance from the Federal Trade Commission (FTC), the nation's consumer protection agency, can help you make smart, sound decisions.

Check federal and state laws or regulation for any specific requirement for your business.

NOTIFYING LAW ENFORCEMENT

When the compromise could result in harm to a person or business, call your local police department immediately. Report your situation and the potential risk for identity theft. The sooner law enforcement learns about the theft, the more effective they can be. If your local police are not familiar with investigating information compromises, contact the local office of the FBI or the U.S. Secret Service. For incidents involving mail theft, contact the U.S. Postal Inspection Service. Check the blue pages of your telephone directory or an online search engine for the number of the nearest field office.

NOTIFYING AFFECTED BUSINESSES

Information compromises can have an impact on your businesses other than yours, such as banks or credit issuers. If account access information – say, credit card or bank account numbers – has been stolen from you, but you do not maintain the accounts, notify the institution that does so that if can monitor the accounts for fraudulent activity. If you collect or store personal information on behalf of other business, notify them of any information compromise, as well.

If names and Social Security numbers have been stolen, you can contact the major credit bureaus for additional information or advice. If the compromise may involve a large group of people, advise the credit bureaus if you are recommending that people request fraud alerts for their files. Your notice to the credit bureaus can facilitate customer assistance.

Equifax
U.S. Customer Services
Equifax Information Services, LLC
Phone: 1-800-685-1111
Email: businessrecordsecurity@equifax.com

Experian
Experian Security Assistance
P.O. Box 72
Allen, TX 75013
Email: BusinessRecordsVictimAssistance@experian.com

TransUnion
Phone: 1-800-372-8391

If the information compromise resulted from the improper posting of personal information on your website, immediately remove the information from your site. Be aware that Internet search engines store, or “cache,” information for a period of time. You can contact the search engines to ensure that they do not archive personal information that was posted in error.

NOTIFYING INDIVIDUALS

Generally, early notification to individuals whose personal information has been compromised allows them to take steps to mitigate the misuse of their information. In deciding if notification is warranted, consider the nature of the compromise, the type of information taken, the likelihood of misuse, and the potential damage arising from misuse. For example, thieves who have stolen names and social Security numbers can use this information to cause significant damage to a victim's credit record. Individuals who are notified early can take some steps to prevent or limit harm.

When notifying individuals, the FTC recommends that you:

- consult with your law enforcement contact about the timing of the notification so it does not impede the investigation.

- designate a contact person within your organization for releasing information. Give the contact person the latest information about the breach, your response, and how individuals should respond. Consider using letters, websites, and toll-free numbers as methods of communication with those whose information may have been compromised.

It is important that your notice:

- describes clearly what you know about the compromise. Include how it happened; what information was taken, and, if you know, how the thieves have used the information; and what actions you have taken already to remedy the situation. Explain how to reach the contact person in your organization. Consult with your law enforcement contact on exactly what information to include so your notice does not hamper the investigation.

- explains what responses may be appropriated for the type of information taken. For example, people whose Social Security numbers have been stolen should contact the credit bureaus to ask that fraud alerts be placed on their credit reports.

See www.ftc.govidtheft for more complete information on appropriate follow-up after a compromise.

- includes current information about identity theft. The FTC's website at www.ftc.gov/idtheft has information to help individuals guard against and deal with identity theft.

- provides contact information for the law enforcement officer working on the case (as well as your case report number, if applicable) for victims to use. Be sure to alert the law enforcement offices working your case that you are sharing this contact information. Identity theft victims often can provide important information to law enforcement. Victims should request a copy of the police report and make copies for creditors who have accepted unauthorized charges. The police report is important evidence that can help absolve a victim of fraudulent debts.

- encourages those who discover that their information has been misused to file a complaint with the FTC at www.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338). Information entered into the Identity Theft Data Clearinghouse, the FTC's database, is made available to law enforcement.

MODEL LETTER

The letter is a model for notifying people whose names and Social Security numbers have been stolen. In cases of stolen Social Security numbers, it is important that people place a fraud alert on their credit reports. A fraud alert may hinder identity thieves from getting credit with stolen information because it is a signal to creditors to contact the consumer before opening new accounts or changing existing accounts. Potential victims of a theft also should review their credit reports periodically to keep track of whether their information is being misused. For some victims, weeks or months may pass between the time the information is stolen and the time it is misused.

FOR MORE INFORMATION

This publication provides general guidance for an organization that has experienced information compromised. If you would like more individualized guidance, you may contact the FTC at idt-brt@ftc.gov. Please provide information regarding what has occurred, including the type of information taken, the number of people potentially affected, your contact information, and contact information for the law enforcement agent with whom you are working. The FTC can prepare its Consumer Response Center for calls from the people affected, help law enforcement with information from its national victim complaint database, and provide you with additional guidance as necessary. Because the FTC has a law enforcement role with respect to information privacy, if you prefer to seek guidance anonymously, you may do so.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

YOUR OPPORTUNITY TO COMMENT

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to www.sba.gov/ombudsman.

MODEL LETTER FOR THE
COMPROMISE OF SOCIAL SECURITY NUMBERS

Dear_____:

We are contacting you about a potential problem involving identity theft. [Describe the information compromise and how you are responding to it.]

We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review.

Equifax	Experian	TransUnionCorp
800-685-1111	888-397-3742	800-680-7289

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call [insert contact information for law enforcement] and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the FTC at www.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforces for their investigations.

We have enclosed a copy of *Take Charge: Fighting Back Against Identity Theft,* a comprehensive guide from the FTC to help you guard against and deal with identity theft.

[Insert closing]
Your Name

INNOVATION IN ACTION UPDATES ON CRITICAL ISSUES AND CHANGES IN THE LAWS AFFECTING YOUR BUSINESS

The FTC's "Red Flag Regulations" To Combat Identity Theft Go Into Effect On November 1, 2008

In 2003, Congress enacted sweeping amendments to the Fair Credit Reporting Act known as the Fair and Accurate Credit Transactions Act ("FACTA"). One of the principal purposes of FACTA is to combat the growing problem of identity theft.

FACTA contains several mechanisms to address identity theft. These requirements, which are set forth in 15 U.S.C. §§ 1681 m(e) and 1681c(h), mandate that:

- Financial institutions and other creditors develop and follow comprehensive policies to identify and prevent identity theft.

- Credit card issuers develop and follow policies for issuing additional or replacement cards in response to a request for such cards made shortly after a change of address notice is received.

- Users of consumer reports develop and follow procedures to verity the identity of a consumer when the address given by the consumer substantially differs from the address contained in the consumer report.

Congress left the job of defining the precise contours of the law to a group of regulatory agencies, including the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the National Credit Union Administration and the Federal Trade Commission. These agencies have now issued joint and final rules and guidelines for compliance with §§ 114 and 315 of FACTA, which are known as the "Red Flag Regulations." The Red Flag Regulations take effect on November 1, 2008.

Who is subject to and must comply with the Red Flag Regulations?

The regulations apply to (1) every financial institution or creditor that offers or maintains "covered accounts," (2) credit card issuers and (3) users if consumer reports. Covered accounts include typical consumer accounts, such as mortgage and auto loans, checking accounts, credit card accounts etc.

What are some of the thing that entities subject to the Red Flag Regulations must do to comply?

All financial institutions and creditors who offer covered accounts must develop and implement a program designed to detect, prevent and mitigate identity theft

in connection with the opening or operation of those accounts. There are four basic elements that must be included in any compliance program.

(1) Identifying relevant "red flags" for covered accounts and incorporating those red flags into an identity theft prevention policy. A red flag is a pattern, practice or specific activity that indicates the possible existence of identity theft. Examples of red flags include the following:

- A fraud or active duty alert include on a consumer report.
- A notice of "credit freeze" on a consumer report.
- A consumer reporting agency providing a notice of address discrepancy.
- Documents provided by the consumer that appear to have been altered or forged.
- The failure of the consumer opening the covered account to provide all required personal identifying information on an application.
- The use of a covered account in a manner that is not consistent with established patterns of activity on the account.
- The use of a new revolving credit account in a manner commonly associated with know patterns of fraud, including the use of a majority of the available credit for cash advances or merchandise that is easily convertible to cash, such as jewelry.
- The return of mail sent to the consumer as undeliverable, although transactions continue to be conducted in connection with the account.

(2) Detecting red flags that have been incorporated into the program. In other words, the financial institution or credit grantor must have in place a plan to check for the red flags of identity theft.

(3) Responding appropriately to red flags that are detected.

(4) Ensuring that the program is updated periodically to reflect changes in risk to customers.

Credit card users must establish and implement reasonable policies and procedures to assess the validity of address changes that are followed by a request for additional or replacement cards. The new or replacement cards may not be issued until:

- The card issuer clearly and conspicuously notifies the cardholder at his/her former address (or by other means of communication previously agreed to) and provides the cardholder with a

reasonable means of promptly reporting incorrect address changes; or

- The card issuer otherwise assesses the validity of the address in accordance with the policies and procedures established as a part of its program.

Users of consumer reports must:

- Develop and implement reasonable policies and procedures that enable them to form a "reasonable belief" that the consumer report relates to the consumer about whom it requested the report when the user receives a notice of address discrepancy.

- Under certain circumstances, develop and implement policies and procedures for furnishing an address that it has reasonable confirmed is accurate to the consumer reporting agency that provided the notice of address discrepancy.

What are the penalties for failure to comply with the Red Flag Regulations?

Financial institutions covered by the Red Flag Regulations are subject to oversight by the appropriate federal banking regulators, which may impose penalties consistent with their regulatory authority.

For those creditors that are not federally regulated financial institutions, the Federal Trade Commission provides oversight. In the event of a knowing violation, which constitutes a pattern or practice of violations, the FTC may commence a civil action to recover a civil penalty in a federal district court. Penalties imposed by the FTC for violations of FACTA may not exceed $2,500 per infraction.

In addition to regulatory enforcement actions, users of consumer reports who fail to comply with the address discrepancy regulation are subject to civil liability under §§ 616 and 617 of the Fair Credit Reporting Act.

The information contained in this Legal alert is not intended as legal advice or as an opinion on specific facts. For more information about these issues, please contact the author(s) of this Legal alert or your existing firm contact.

Name	Telephone	Email	Office
Craig E Bertschi	(404) 815-6493		Atlanta

The invitation to contact the author is not to be construed as a solicitation for legal work. Any new attorney/client relationship will be confirmed in writing. Your can also contact us through our web site at www.kilpatrickstockton.com

Code of Conduct

Code of Conduct: Purpose

The mission of each and every employee of **Action Recovery & Collections LLC** is to serve the needs of our clients and their customers with respect, integrity, and always within laws and regulations governing our industry. **Action Recovery & Collections LLC** has established a code of conduct setting forth principles and guidelines with respect to ethics and integrity expected to be followed at all times when representing **Action Recovery & Collections LLC**. The following code of conduct is to be read, understood, and signed as a condition of employment with: **Action Recovery & Collections LLC**

Action Recovery & Collections LLC Mission Statement

Action Recovery & Collections LLC is a nationally recognized firm focused on providing Asset Management and Recovery Services to financial and commercial customers. We are committed to our customer's complete satisfaction as we help them profitably manage their accounts receivable. Our goal is to partner with our customers by providing what they want, when they want it properly and cheerfully. On a scale of 1-10, we expect to rate a 10!

Our reputation in the marketplace is defined by our Service, Integrity, and Results.

We will measure our success in terms of our clients' satisfaction. We will seek out the expected results that each individual client requires of our partnership and we will hold ourselves accountable to delivering these results, whatever they may be, to the level of excellence that delights our customers.

Our vision is to be the best company, to be the best employee, and to be the best person! This has been the tradition of our company, this is what our clients deserve, and this is what makes **Action Recovery & Collections LLC** superior to our competition.

Vision Statement

Our vision is to be the best company, to be the best employee, and to be the best person!

Third Party Disagreement / Problem Report

Open Date:	Time:	Resolved Date:	Log #:

Name of initial contact person (if applicable)		Account #	
Name of Supervisor Taking Call:		Client:	
Supervisor Assigned To:		R/P Name:	
Third Party Name:		Third Party Attorney's Name (if applicable):	

NATURE OF THIRD PARTIES DISAGREEMENT / PROBLEM

✓ Agency Related	✓ Identity Related	✓ Payment Related	✓ Client Related
☐ Agent's Attitude	☐ Wrong Party	☐ Balance	☐ Defective Goods or Unauthorized Charge
☐ Recovery Practice (phone)	☐ Consumer Responsibility	☐ Billing Error	
☐ Recovery Practice (face to face)	☐	☐ Charge or fees	☐ Disputed
☐ Good Recovery Call	☐	☐	☐ Obsolete Debt
☐	☐	☐	☐ Insurance

Remarks: Describe Incident

ACTION TAKEN (if any):

Corrective Action Req.?		If Yes, Targeted Resolution Date		Corrective Action No.	

Employee Confidentiality Agreement

COMPANY EMPLOYEE CONFIDENTIALITY AGREEMENT

I, _____ acknowledge and agree that I will not disclose, disseminate, publish or in any way compromise the integrity of any confidential information to which I have access by virtue of my employment with **Action Recovery & Collections LLC**. I understand that "Confidential Information" includes, but is not limited to:

- consumer reports and related data
- protected healthcare information
- proposals
- billing status/financial data
- personnel files (for other employees)
- research and development
- Consumers' accounts – anything related
- price list
- computer programs
- technological data
- marketing plans
- business and trade secrets
- client lists

I acknowledge and agree that in the event that I violate this Employee Confidentiality Agreement, I may be disciplined or terminated and that civil and /or criminal action may be taken against me for which I may be personally liable.

I acknowledge that I have been trained and understand all aspects of FDCPA, FCRA, FACTA, GLBA, TCPA and TRPPA and will be in compliance with all company procedures related to these laws.

I acknowledge that my employment with **Action Recovery & Collections LLC** is contingent upon my execution of and compliance with Employee Confidentiality Agreement. I also understand that this **Employee Confidentiality Agreement is not a contract for employment** and does not in any way alter the at-will nature of my employment which is such that I or **Action Recovery & Collections LLC** may terminate my employment at any time.

_____

Signature

Confidentiality and Non-Disclosure Agreement

Organizational information that may include, but is not limited to, financial, consumer identifiable, employee identifiable, intellectual property, financially non-public, contractual, including without limitation information of a competitive advantage nature, and from any source or in any form (i.e., paper, magnetic or optical media, conversations, film, etc.), may be considered confidential. It is my job to preserve information's confidentiality and integrity as well as maintain its availability. The value and sensitivity of information is protected by law and by the strict policies of **Action Recovery & Collections LLC** (sometimes called the "Company").

The intent of these laws and policies is to assure that confidential information will remain confidential through its use, only as a necessity to accomplish the company's mission.

As a condition to receiving a computer sign-on code and allowed access to a system, and/or being granted authorization to access any form of confidential information identified above, I, the undersigned, agree to comply with the following terms and conditions:

1. My Sign-On Code is equivalent to my LEGAL SIGNATURE and I will not disclose this code to anyone or allow anyone to access the system using my Sign-On Code.

2. I am responsible and accountable for all entries made and all retrievals accessed under my Sign-On Code, even if such action was made by me or by another due to my intentional or negligent act or omission. Any data available to me will be treated as confidential information.

3. I will not attempt to learn or use another's Sign-On Code.

4. I will not access any on-line computer system using a Sign-On Code other than my own.

5. I will not access or request any information I have no responsibilities for. In addition, I will not access any other confidential information, including personnel, billing, financial, health or other private information I do not need to perform the duties assigned me by the Company or its client.

6. If I have reason to believe that the confidentiality of my User Sign-On Code/password has been compromised, I will immediately change my password and notify our company's security administration area.

7. I will not disclose any confidential information unless required to do so in the official capacity of my employment or contract. I also understand that I have no right or ownership interest in any confidential information.

8. I will not leave a secured computer application unattended while signed on.

9. I will comply with all policies and procedures and other Company rules about the confidentiality of information and Sign-On Codes.

10. I understand that my use of the system will be periodically monitored to ensure compliance with this agreement.

11. I agree not to use the information in any way detrimental to the Company and will keep all such information confidential.

12. I will not disclose protected information or other information that is considered proprietary, sensitive, or confidential unless there is a need to know basis or unless I am otherwise required by law to do so.

13. I will limit distribution of confidential information to only parties with a legitimate need in performance of our Company's mission.

14. I agree that disclosure of confidential information is prohibited indefinitely, even after termination of employment or business relationship, unless specifically waived in writing by the authorized party.

15. This agreement shall survive the termination, expiration, or cancellation of this agreement or my employment at the Company.

I further understand that if I violate any of the above terms, I may be subject to disciplinary action, including discharge, loss of privileges, termination of contract, legal action for monetary damages or injunction, or both, or any other remedy available to the Company or its clients.

User's Name_____

Date: _____
(Please Print)

User's Signature_____

If I have any questions about this document or the policies and procedures it mentions, I will notify my immediate supervisor, a compliance officer, or another manager and seek assistance.

Computer Usage Agreement

- All hardware (includes owned and not owned by **Action Recovery & Collections LLC)** used to access the **Action Recovery & Collections LLC** network must be used only for **Action Recovery & Collections LLC** business.

- **Action Recovery & Collections LLC** must approve all hardware purchased with **Action Recovery & Collections LLC** funds.

- **Action Recovery & Collections LLC** must approve all hardware not owned by **Action Recovery & Collections LLC** that is used to access the **Action Recovery & Collections LLC** network.

- Internet and email usage will only be for **Action Recovery & Collections LLC** business and is subject to monitoring.

- **Action Recovery & Collections LLC** must approve all software loaded onto hardware owned by **Action Recovery & Collections LLC** or any piece of hardware used to access the **Action Recovery & Collections LLC** network. This includes wallpaper screensavers, music downloads, or any other piece of software.

I agree to comply with **Action Recovery & Collections LLC** computer usage policy at all times, or otherwise approved by **Action Recovery & Collections LLC,** with the understanding that **Action Recovery & Collections LLC** will periodically scan assets for viruses and unauthorized software. I understand that if I violate the policy, I may be subject to further disciplinary action up to and including termination. In addition, I acknowledge if necessary, **Action Recovery & Collections LLC** will advise appropriate legal officials of any illegal violations.

_____

Employee Name (Please Print)

_____

Employee Signature Date

_____

Supervisor/Manager Signature Date

Minimum Necessary Rule

RESPONSIBILITY: Privacy Official or Compliance Officer

BACKGROUND;

Protected Non-Public Personal Information (NPPI) must be treated with the utmost confidentiality. Members of the **Action Recovery & Collections LLC** workforce are required to limit the amount of protected information they use, request, or disclose to others, to the minimum amount necessary to achieve the specific purpose of that use, request, or disclosure.

This policy establishes the general rule regarding the *minimum necessary* limitation on the use or disclosure of protected information.

POLICY;

Members of the **Action Recovery & Collections LLC** workforce may not use, request, disclose to others, any protected health information that is more than the minimum necessary to accomplish the purpose of the use, request, or disclosure.

Members of the workforce are required to comply with specific policies and procedures established to limit used of, requests for, or disclosures of protected health information to the minimum amount necessary.

> **Exception.** **Action Recovery & Collections LLC** is not limited in the amount of protected information that it may disclose to the Consumer.

When federal or state law requires a disclosure of protected information, the minimum necessary amount of information is that which is required in order to comply with such law.

When disclosing a consumer's own information to that consumer, the minimum necessary rule does not apply.

Compliance Procedures

Written Consumer Disputes Concerns and Issues

1.0 PURPOSE

This procedure is to ensure all consumer, approved third party, or consumer's attorney disputes are handled in accordance with the Fair Debt Collection Practices Act (FDCPA), the Fair Credit Reporting Act (FCRA), state laws and regulations and the company's philosophies.

2.0 SCOPE

This procedure applies to all company personnel who deal with written consumer or consumer's attorney disputes.

3.0 DEPARTMENTS RESPONSIBLE FOR IMPLEMINTATION

3.1 Director of Compliance (DOC)

3.2 Compliance Assistant (CA)

3.3 Recovery

3.4 Client Services

4.0 GENERAL

4.1 All written disputes are directed to the Director of Compliance / Compliance Assistant for review.

4.2 DOC or CA will log the issue in an appropriate manner.

4.3 DOC or CA will fill out third party disagreement report when necessary.

4.4 If it is determined to continue collection of the debt, a written response is prepared and sent to the consumer, approved third party or consumer's attorney by the DOC or CA assigned.

4.5 If the consumer, approved third part or consumer's attorney writes that we cease all communications and recovery efforts, or write that they will not pay the debt, all precautions are taken to ensure we never contact the consumer or consumer's attorney again.

4.6 If it is determined that it is not beneficial to respond to the dispute, the account will be returned to the client as disputed.

5.0 PROCEDURE

5.1 The person opening the mail will direct all written disputes to the DOC or CA as appropriate.

5.2 The DOC OR CA

5.2.1 Will notate the account describing the consumer or consumers attorney's dispute and review the dispute

5.2.2 Will fill out third party disagreement report when necessary and direct the issue to the employee's manager (if applicable)

5.2.3 Will log dispute in an appropriate manner.

5.2.4 Disputes requesting the agency to cease communications the DOC or CA will:

- Return the account to the client as a disputed account; or
- Cease any and all recovery attempts
- Flag all phone numbers as do not call numbers;
- Notate account with dispute information;
- Indicate we are to cease communication and recovery efforts with the consumer or consumer's attorney;
- Review account to determine if this is a good prospect for legal action;
- Request the consumer reporting agency to flag the account as disputed on the consumer's credit report; and
- Image the dispute letter.

5.2.5 Disputes requesting verification of the debt the DOC or CA assigned to the claim will:

- Obtain a complete and accurate Itemized Statement either electronically or from Client Services and send it to the consumer, approved third party or consumer's attorney.

5.2.6 Specific disputed requiring client resolution the DOC or CA assigned will turn over the Client Services to obtain the pertinent information

5.2.7 Work with Client Services and the client to investigate the dispute and obtain any necessary information including a complete and accurate itemized statement

5.2.8 Formulate a written response to mail with the itemized statement

5.2.9 Disputes determined to be valid or the balance does not warrant extensive investigation, the Compliance Manager or CA will return the account to the client as disputed

6.0 RECORDS

A digital image of the written dispute and, if applicable, the written response is attached to the consumer's account. Third party disagreement report log is maintained by QA for 12 months.

7.0 FORMS

7.1 CF_806-1	Third Party disagreement/Problem Report
7.2 CF_806-3	Third Party Disagreement Compliance Log Worksheet
7.3 CF_806-6	Agency Compliance Log Worksheet

Third Part Disagreements

1.0 PURPOSE

This procedure is to ensure all verbal consumer, consumer's attorney, or third party disagreements are handled in accordance with the Fair Debt Collection Practices Act (FDCPA), the Fair Credit Reporting Act (FCRA), state laws and regulations and the company's philosophies.

2.0 SCOPE

This procedure applies to all company personnel who deal with verbal consumer, consumer's attorney, or third party disagreements.

3.0 DEPARTMENTS RESPONSIBLE FOR IMPLEMENTATION

3.1 Quality Assurance

3.2 Direct of Compliance

3.3 Department Manager

3.4 All Staff

4.0 GENERAL

4.1 When a claim escalates to Manager/Supervisor, the Manage/Supervisor will complete the third Party Disagreement/Problem Report. It is then given to Quality Assurance.

4.2 Quality Assurance logs and turns the dispute over to appropriate Department Manager. Upon total resolution will shred all Third Party Disagreements.

4.3 Department Manager determines if corrective action is necessary and initiates follow-up. Will present closed Third Party Disagreements at regularly scheduled meeting.

5.0 PROCEDURE

5.1 The Third Party disagreement/Problem Report is completed by the Manager/Supervisor taking the escalated call and given to Quality Assurance.

5.2 Department Manager/Supervisor taking the escalated call.

5.2.1 Will notate the account in FACS describing the consumers, consumer's attorneys or third party disagreement.

5.2.2 Will listen to the call if available, coach and mentor the Recovery Agent.

5.2.3 Will fill out the Third Party Disagreement/Problem Report and submit the report to Quality Assurance.

5.2.4 Will work with Client Services and/or Sales if the disagreement needs resolution from the client when applicable.

5.2.5 Will attend regularly scheduled monthly meetings.

5.3 Quality Assurance

5.3.1 Will log the disagreement on the Third Party Disagreement Log.

5.3.2 Will direct the Third Party Disagreement to the employee's manager.

5.3.3 Log the resolution date of the Third Party Disagreement and shred all Verbal Third Party Disagreements once the disagreement has been discussed in the monthly meeting.

5.3.4 Will coordinate the monthly meeting so the Supervisor or Manager who took the call can present third party disagreements.

5.4 Department manager

5.4.1 Will review the Third party Disagreement.

5.4.2 Will determine if corrective action is required.

5.4.3 Will attend all regularly scheduled monthly meetings.

5.4.4 Upon resolution of a Third Party Disagreement, will be present and discuss solutions at scheduled monthly meetings when the original Supervisor or individual that took the call is not in attendance.

Will return Third Party Disagreements to Quality Assurance with a resolution date.

6.0 RECORDS

The Third Party Disagreement/Problem Reports are shredded when deemed obsolete. The Consumer Dispute log is maintained by Quality Assurance for 12 months.

7.0 FORMS

7.1 CF 806-1 Third Party Disagreement/Problem Report

7.2 CF 806-3 Third Party Disagreement compliance Log Worksheet

7.3 CF 806-6 Agency Compliance Log Worksheet

7.4 CF 1201-1Non-Conformity Log

Compliance with Recovery Regulations

1.0 PURPOSE

The purpose of this procedure is to give direction on following recovery regulations.

2.0 SCOPE

This procedure applies to recovery regulations for FDCPA, FCRA, HIPPA and all other state and federal laws and regulations.

3.0 DEPARTMENTS RESPONSIBLE FOR IMPLEMENTATION

3.1.1 ALL

4.0 GENERAL

All employees must be educated in and educated in and follow the requirements of any and all recovery agency regulations.

5.0 PROCEDURE

5.1 All employees will adhere to the requirements of:

5.1.1 The Fair Debt Collection Practices Act (FDCPA)

5.1.2 The Fair Credit Reporting Act (FCRA)

5.1.3 Gramm-Leach-Bliley Act (GLBA)

5.1.4 All other applicable state and federal laws

5.2 Compliance:

5.2.1 Will notify all employees of any changes in the regulatory requirements and update all reference materials used by **Action Recovery & Collections LLC** staff.

5.2.2 Have all notices in use reviewed and approved as compliant with regulatory requirements by our company attorney.

5.2.3 Inspect automated processes (i.e., Credit Bureau Reporting, Written disputes and Direct disputes via e-Oscar) to ensure compliance with all regulatory requirements.

5.2.4 Will Update Trainers of any new laws.

5.3 Training will:

5.3.1 Hold regular training classes to review laws.

6.0 RECORDS

All records are maintained in accordance with Management of Records and Data.

7.0 FORMS

7.1 CF 807-1 Credit Bureau Data Change Form

7.2 CF_806-2 CONSUMER DISPUTE LOG

7.3 CF_806-3 THIRD PARTY DISAGREEMENT COMPLIANCE LOG WORKSHEET

7.4 CF_806-6 AGENCY COMPLIANCE LOG WORKSHEET

Assignment of Access Privileges

RESPONSIBILITY: Director of Information Systems, Chief of Operations

BACKGROUND:

Not all members of the **Action Recovery & Collections LLC** workforce need to have access to all protected information or non-public financial information about consumers. Our Agency assigns minimum access profiles to all job titles on the basis of how much information, pertaining to which types of claims, is needed to accomplish work assignments.

These access profiles are used for two purposes:

1. For NPPI that is entered or stored electronically, the access *profile* determines which information an individual member of the workforce may read through a computer terminal.

2. Also, access profiles are incorporated into job descriptions and training materials so that all members of the workforce will know which protected information, whether electronic or not, they are permitted to see or use. A supervisor may request that an access profile be expanded, creating a new access profile, for a member of the workforce who has a greater 'need to know," based upon additional job responsibilities.

POLICY:

Action Recovery & Collections LLC will maintain access profiles to specify which protected information may be used by workforce members in each job class. These profiles will specify the data elements that comprise protected information.

Access profiles are based upon two principles: First, that access to information must not be so restricted as to interfere with the quality or efficiency of Access profiles will comply with the MINIMUM NECESSARY RULE.

Access profiles will be used to limit electronic access to protected information.

Access profiles will also be incorporated into job descriptions and training materials, to assure that each member of the workforce is aware of what information he or she may and may not see and use.

Access profiles will include types of information (e.g., personal, financial, or demographic), types of consumers (e.g., from a particular area, at a particular site, or from any restricted site), dates of service (e.g., within this month, or paid in last 90 days), and other pertinent identifiers that define which data may or may not be read.

Upon successful demonstration of need, a specific access profile may be modified for members of the workforce who have a demonstrated need to read additional information to accomplish their work assignments.

Access profiles will be reviewed and revised annually, or upon request of a member of management when a new job is created, when a job or class of jobs changes significantly, or when experience shows a need to make a modification.

PROCEDURE;

1. An ad hoc access profile committee will be comprised of the following, or their designees;

    - Director of Information Systems *(chair)*
    - Designated Privacy Official
    - Designated Security official
    - Chief of Operations

2. The ad hoc access profile committee will

    - Review job descriptions and assign them to job classes, based on the NPPI required to accomplish the job efficiently.
    - Assign NPPI data elements to categories
    - Assign categories of NPPI to job categories, to form access profiles
    - Review access profiles annually, or when requested
    - Have new access profiles and job classifications reviewed by managers to whom the affected jobs report, and make such changes as are warranted to satisfy the two principles of quality and efficient care and patient privacy.

3. The Human Resource Coordinator will incorporate each job's access profile into the job description and into training materials, to assure that each member of the workforce is aware of what information he or she may see and use, and which he or she is not permitted to see or use.

4. The Director of Information Systems will assure that members of the workforce have electronic access to NPPI that is consistent with their access profiles. Records of how this is achieved will be retained for as long as a given access profile is in effect, until the date it is supplanted by a revised profiled, plus six years.

5. Job classes, NPPI classification, access profile composition, and access profile assignments will be recorded. The record will include brief descriptions of the rationale behind classification and assignment decisions. Each of these records will be kept for six years after the date it is superseded by a revision.

6. In situations where a member of the workforce requires additional access based upon work assignments, that person's supervisor may submit a request for modification of that employee's access profile. All requests should include evidence of additional responsibilities and training to support the need for modified access.

7. The access profile committee will keep minutes. Minutes will be retained for six years.

RATIONALE:

Action Recovery & Collections LLC may use role-based *access control*, while recognizing that, in some circumstances, a person's job may be so unique as to constitute a role in its own right.

Job and data classification if entrusted to a committee representative of the principal areas of expertise necessary to achieve the objective of this classification system.

Two principles guide the development of access profiles: the quality and efficiency of claim management, and the privacy and security of consumer information.

The same access profiles are used to develop electronic access controls, and training and job standards, to guide access to any NPPI in whatever medium: paper, voice, electronic, or other medium.

See also: MINIMUM NECESSARY RULE
ROUTINE AND RECURRING DISCLOSURES OF PROTECTED NON PUBLIC PERSONAL INFORMATION

NPPI Security P&P Checklist					
	Have it already?	Is it current?	GLBA compliant	Updated?	Training done?
1. General Guidelines to Safeguard Protected Information					
2. Risk Analysis and Ongoing Risk Management					
3. Sanctions for Violation Privacy and Security Policies and Procedures					
4. Activity Review of Information System Security					
5. Assignment of Security Responsibility					
6. Assignment and Management of Information Access Privileges					
7. Termination or Modification of access to Protected Information: Facility Controls and Electronic Systems					
8. Training Program: Security Awareness and Training to Safeguard Electronic Protected Information					
9. Security Incident Procedures: Response and Reporting					
10. Contingency Planning: Response to Unexpected Negative Events					
11. Evaluation of the Security of Protected Information					
12. Business Associates Contracts and Other Arrangements					
13. Maintenance of Privacy and Security Policies and Procedures					
14. Assignment of Facility Access Controls or Privileges					
15. Policies and Guidelines on Work Station Use and Security					
16. Device and Media Controls					
17. Access Control					
18. Audit Controls					
19. Integrity					
20. Authentication of Person or Entity					
21. Electronic Transmission Security of PHI					
22. E-Mail and Protected Information					
23. Facsimile Machines and Protected Information					

Written Disputes

Description: Working guide to receiving, processing, and following up on written disputes from consumers and their attorneys. Also includes description of common dispute types, as well as the time deadlines associated with each type as outlined in the FDCPA and FCRA.

Scope: Applicable to any written correspondence from consumers, attorneys, and authorized third parties that contains dispute language.

System Used: FACS (DEF, BEL, SEN), FACSWORD.

Who is Responsible: This process is interdepartmental, and is networked between Business Support, Compliance, and Client Services.

Frequency of work: Daily

Important Information

An understanding of the implications of FDCPA and FCRA as they pertain to written disputes is a key part of this process, so please read the following carefully.

FDCPA

For the purposes of this instruction, the FDCPA applies as follows:

a. Any dispute received and postmarked within 30 days of the initial validation notice ***must*** be verified unless we are ceasing all recovery efforts.
b. There is no time period within which the debt must be verified.
    i. It is the opinion of the Compliance Department that a consumer is unlikely to pay the debt without verification.
c. A dispute received at any time must be reported to the consumer reporting agency.
d. When an account is placed into XDIS or X5DS FACS automatically stamps the account as disputed.

For the purposes of this instruction, the FCRA applies as follows:

a. **Action Recovery & Collections LLC** has a duty to perform a reasonable investigation upon receiving an inquiry regarding what is being reported to the consumer reporting agency.
b. The investigation and response to the inquiry must be completed within 30 days of receipt of the inquiry.
c. It ***is not*** necessary to provide an itemized statement in response to the inquiry.
d. It ***is*** necessary to mark the account as disputed.

Procedure

Once received and scanned by Business Support Representative, disputes will be forwarded to the Compliance Assistant.

1. **FACS operation**

    a. Enter menu 8.1.1 or 7.1.1 depending on access.
    b. Located the account number and enter it at the account prompt.
        - Be sure that the dispute is being worked in the correct directory (DEF, BEL, OR SEN).
    c. Verify that the dispute has been imaged in the **47** or **IM** window.
    d. Verity that the name in the responsible party field matches the name on the dispute.
        - If the dispute is from an attorney, verity that the correspondence references the responsible party, or the attorney who is listed in the **22** or **DA** window.
            - If attorney who wrote the letter is dispute is not listed in the **22** or **DA** window, list them there and place an "H" on all phone fields.

2. **"Slot" the dispute**

    a. Read the dispute in its entirety, being sure to note any attached documentation (i.e., copies of cancelled checks, EOB's client correspondence, etc.).
    b. Determine the reason the account is being disputed and refer to the instructions contained in the corresponding "slot" in Appendix i: Dispute Types*

3. **Complete the 666 window (if applicable)**

    a. If the account needs further attention from Client Services be sure to leave written instructions in the **666** window.
        - **Note:** A synopsis of the dispute is not necessary at this juncture of the process, simply detail the steps to be followed by the Representative once they receive the account.
    b. Fill in the "Request Type:" field at the bottom of the window with the number that corresponds to the reason the account is being forwarded to Client Services.

4. **Notate FACS**

    a. Once the steps outlined in *Appendix i* have been completed, created a note in the **8** or **N** window detailing the contents of the dispute correspondence and what action was taken.
    b. Also note any new location information included within the correspondence.
    c. Place the account in the proper disposition with the appropriated wait date as outlined in *Appendix i.*

5. Update the dispute Log

a. The log is contained in **(Your File Code)** \Company\Disputes.
b. Locate the account number in the "Dispute Image to Account #:" column.
c. Fill in the "Dispute Reviewed By:" column with initials.
d. Fill in the "Date:" column with the date the dispute was worked.
e. Save and close log once finished.

6. Shred documents.

a. Shred all dispute correspondence including attachments

*For a visualization of the Dispute Process, and a list of letters used, see appendices ii – iii

Appendix: Dispute Types

When step 2 of the Procedure process has been completed, match up the dispute with the corresponding list of dispute types below. Consider the language, intent or implied request, and the "spirit" of the FDCPA and FCRA when taking any action on a dispute. If unable to it a particular dispute into a single slot, or any slot at all, submit it to Compliance for review.

Dispute Type	Who Handles the Dispute and How
"Standard" dispute includes "I dispute" somewhere, or is a form letter mentioning a "confusing item" on a consumer report or "I am informed that your company must provide verification…"	• Received **within 30 days** of list: Make a note in the **666** window that an itemized statement needs to be sent to the consumer. Place the account in X5DS with no wait date, and Client Services will respond. • Received **outside 30 days** of list: Send the balance due letter (201) to the consumer. Return the account to last known call disposition with a wait date of 30 days.
Repeated disputes written either directly to ABC or to the consumer reporting agencies via E-Oscar, without any new information	If a consumer continually sends disputes, refer to the guidelines listed in *Appendix iii:* Letter List. If letters regarding the dispute have been sent previously, simply note FACS that another letter of dispute was received, place in last call disposition and log the dispute.
Paid in full claims consumer states balance been paid previously	Make a note in the **666** window stating that consumer made the claim, and include any proof of payment information included (check number, date, amount, etc.) Place account into X5DS with no wait date, where it will be reviewed by Client Services and verified with the client.
Disputing based on insurance consumer states insurance was never billed, billed incorrectly, etc.	Notate any new insurance information in the **667** window (insurance cards, Medicare/Medicaid numbers, etc.) Make note in the **666** window stating new insurance information is available and place the account in S5DS with no wait date.

Client issues consumer states won't pay due to negligence in services provided, threatening to file complaint or legal action against client, etc.	Make a very specific note in the **844** window notifying the client of the contents of the dispute. Keep in mind that the **844** letter pulls directly from this window, so the client will read whatever is printed there. Print the letter and forward it to Client Services.
Identity theft or forgeries consumer claims services were not rendered to them, ID was stolen, never been to client's hospital, etc.	If the dispute contains a police report or supporting documentation of any kind, make a note in the **666** window requesting that the imaged material be reviewed by Client Services, and place the account in X5DS. If no supporting documentation is provided, make a note on the account for a collector to call and ask consumer to forward that information to State. Put in XATT and forward to Collection Supervisor.
Ceases Consumer states wants no more calls, no more correspondence, "stop harassing me," "I refuse to pay," etc.	Place holds on all phone fields using the "!" character not the "H." Place the account in 3600 with no wait date. If balance is large enough and the consumer is employed, place account in 0040 with a 30 day wait date to pursue possible legal action.
Bankruptcies the account is disputed due to bankruptcy filing	Note any bankruptcy information received in the 807 or BANKO window and follow normal bankruptcy procedures. If no information is included, call VCIS to locate it.
Collection practices dispute Consumer is upset by the action of a collector, actions of ABC as a whole, or threatens any sort of recourse against State	Handle any requests or demands the consumer lists as stated in above slots. When finished forward the document to the Compliance Manager who will in turn investigate the claim and open a Third Party Disagreement/Problem. Quality Assurance will then log the Third Party Disagreement/Problem.
Divorce consumer states not responsible due to divorce.	Check to see if date of divorce is included on account or dispute. If it is, determine if consumer or ex-spouse (or both) is responsible. If it is not, check CCAP or forward to Collection Supervisor to have collector call consumer to locate proper information. Make sure to include detailed note in FACS.
Deceased Spouse or third party such as an attorney or family member disputes an account based on the fact that the consumer is deceased	Follow standard probate procedures (see work instruction "Filing A Probate Claim" located in company/ppmsworkinstructions/specialservices).
Miscellaneous consumer states we have wrong person, reporting on incorrect consumer report, divorced, minor on date of service, not responsible, etc.	Forward to Compliance Assistant for review.

System Security

1.0 PURPOSE

The purpose of this procedure is to define security measures within the computer systems.

2.0 SCOPE

This procedure applies to all security issues relating to computer systems used for collection purposes.

3.0 DEPARTMENTS RESPONSIBLE FOR IMPLEMENTATION

3.1 ALL

4.0 GENERAL

4.1 Information Systems will set up new users and remove security at employee termination.

4.2 Department Managers will provide all employees in their department with the minimum security access required to perform their jobs, and this security will be reviewed upon a change in job position.

4.3 Compliance will inform information Systems of any regulatory changes.

4.4 Information Systems will maintain the system security access to comply with regulatory requirements.

5.0 PROCEDURE

5.1 Information Systems will

5.1.1 Set up new employees' workstations with the most basic level of security required to run the workstation.

5.1.2 Set up all new users with the most basic level of security in the FACS system.

5.1.3 Remove workstation and FACS security at time of employee's termination.

5.1.4 Assign user passwords at workstations and in FACS.

5.1.5 Change password after initial setup if necessary.

5.2 Human Resources will

5.2.1 Notify Information Systems when a new user needs to be added to the system.

5.2.2 Notify Information Systems to remove user security at an employee's termination.

5.3 Department Managers/Supervisors will

5.3.1 Determine the minimum security required for each employee to perform their job and assign that security to their own employees.

5.3.2 Only give security to their employee after the employee has been fully trained on how to do the job.

5.3.3 Determine whether security should be removed, or more training is necessary if a non-conformity arises relating to security issues.

5.3.4 Review the employee's security at time their job functions change to ensure they have only the security required to perform their job duties.

5.4 All employees will

5.4.1 Sign the Security Access Request Form when new security is required and give it to their Department Manager.

5.4.2 Be provided with and use the minimum level of system security access required to perform their job duties.

5.4.3 Use the security they are given for only the job functions for which they are responsible.

5.5 Collection Manager will maintain and assign company wide security access to adhere to collection regulatory requirements (i.e., disposition and letter control lists, etc.)

6.0 RECORDS

All Records are kept in accordance with ALL_CP_1401 Management of Records and Data.

7.0 FORMS

7.1 CF_1301-1 Computer Access Request Form

8.0 REFERENCE DOCUMENTS

8.1

Skiptracing and Asset Searching

1.0 PURPOSE

The purpose of this procedure is to provide instructions for management of skiptracing and asset searching actions.

2.0 SCOPE

This procedure applies to all skiptracing and asset searching processes and individuals who participate in the skiptracing and asset searching process.

3.0 DEPARTMENTS RESPONSIBLE FOR IMPLEMENTATION

3.1 Recovery Services Department

3.2 Compliance

3.3 Special Services

4.0 GENERAL

4.1 Acquisition of location information on consumers in the recovery services department.

4.2 Acquisition of location information for our clients who have received returned mail on their customers.

4.2 Adhere to all regulatory requirements.

5.0 PROCEDURE

5.1 Regular Recovery, Financial Recovery and Commercial Recovery, Special Services.

5.1.1 May at any time throughout the recovery process need to locate a consumer's phone number, address or place of employment. Primarily responsible on new business accounts to do this utilizing the work instructions as outlined in the Master Flow Chart.

5.1.2 May utilize specific work queues and pools designed to identify consumers for whom we need to re-establish communication with and recovery of collateral upon those they are able to locate.

5.1.3 Verifies employment for accounts within the special services department so that further post judgment remedies may be taken.

5.2 Recovery Department Supervisors Perform random audits of the recovery services.

5.2.1 Assists in any task given by the Recovery Department Manager in implementing or monitoring any skiptracing or

asset searching function in any of the above named departments involved.

5.3 Compliance

5.3.1 Will ensure all departments adhere to the regulatory requirements (in accordance with COM_CP_807).

6.0 RECORDS

All records are maintained in accordance with Management of Records and Data Procedures.

ARS:	Sally Student
Instructor Name:	
Class Dates:	09-10-07 to 9-28-07

Graduation Requirements
Knowledge Assessments = 85% Overall
Quality Assurance = 75% Overall
FDCPA Requirements = 100% Overall
Scorecard Competencies = 85% (85/100)

System Competencies	Week 1	Week 2	Week 3
Log in/out - Network	2	2	2
Log in/out Account Management System	2	2	2
Log in/out Phone System	2	2	2
Log in/out Dialer	2	2	2
Access accounts via Account inquiry	2	2	2
Identify info on Account Detail Screen	2	2	2
Properly notes accounts	2	2	2
Uses proper transfer procedures	2	2	2
Use correct smart codes	2	1	1
Demonstrates knowlegde of Function "F" keys	2	2	2
Set Client Web Site Payments		2	2
Set up proper Payment Arrangements		2	2
Set up ACH and Credit Card Payments		2	2
Identifies and works linked accounts		2	2
Total	20	27	27

Role Playing Competencies	Week 1	Week 2	Week 3
Demonstrates Communication Skills & Etiquette	2	2	2
Demonstrates and applies FDCPA	2	2	2
Demonstrates eight steps of collection call			
Demonstrates Industry billing practices		2	2
Can handle frauds, disputes, bankrupcy, etc		1	1
Demonstrates knowledge of Client specifics and CIC		2	2
Total	4	9	9

Totals	
ScoreCard	96.0%
Week 1-KA	103%
Week 1-QA %	84%
Week 2-KA	
Week 3-FDCPA	100.0%
Week 3-KA	97.0%
Week 3-QA %	84.0%

ATTENDANCE (2)	
Date	Points

Date	Behavior

Training Log

Training Conducted:	Date:_____
_____ New Refresher Required Optional	**Time:**_____
Instructor:	**Location:**_____
Attendance Roster:	**Attendance Roster:**
1	16
2	17
3	18
4	19
5	20
6	21
7	22
8	23
9	24
10	25
11	26
12	27
13	28
14	29
15	30

*** Attach program outline with learning objectives that meet a specific training need or other documentation on how this training meets criteria tied to your compliance program.**

Compliance Issue Tracking Form

Collections

Quarter End Legal Incidents Reports	**BOLDFACE**	INDICATES NEW ITEM OR STATUS CHANGE
		INDICATES SPECIAL INTEREST ITEM
		INDICATES ITEM TO BE ARCHIVED

Type / Priority	Item #	Party Name	Date Reported	Account Number	Compliance Incident No.	PPMS Issue Number	Case, Filing or Action No.	Nature of Action / Complaint	Deadline (if Applicable)	Current Disposition	Date Closed
Legal Actions											
Regulatory Complaints											
Regulatory Inquiries And Letters											
Atorney Communications & Probate Actions											
Consumer Communications with Legal Issues											
Legal Questions, Contracts Letter Approvals & Analysis Requested by:											
Licenses & Registrations											

Compliance Department Review

Month & Year_____ **{S} = Satisfactory** **{US} = Unsatisfactory**

Compliance	{S}	{US}	Week 1	Week 2	Week 3	Week 4	Week5
E-Oscar–Queue Completed Daily							
Review of Outbound Mail Daily							
Review and Send Collection Faxes Daily							
Process Mail Disputes Daily							
Respond to DFI & Other Govt Inquiries Timely							

Monthly Monitoring Form

Name								
Traits								
Adherence to Policy	The extent to which an employe follows rulles, other regulations, adheres to company and client policy and practice, and to the technical and legal standard of our profession:	January	February	March	April	May	June	6 Month Total
		Rating	Rating	Rating	Rating	Rating	Rating	
		July	August	September	October	November	December	12 Month Total
		Rating	Rating	Rating	Rating	Rating	Rating	
Monthly comments:								
Professionalism								
	The ability of the employee to exhibit a courteous and general business-like manner in the workplace, to our clients, and customers, by conforming to the ethical standards of the profession. The extent to which an employee willingly demonstrates the ability to cooperate, assist, and communicate with peers, subordinates, upper mangement, and clients.	January	February	March	April	May	June	6 Month Total
		Rating	Rating	Rating	Rating	Rating	Rating	
		July	August	September	October	November	December	12 Month Total
		Rating	Rating	Rating	Rating	Rating	Rating	
Monthly Comments:								

Third Party Disagreement Compliance Log Spreadsheet

Log #	Date discussed	Date Received	Employee taking complaint	Agency staff	Employee assigned to	Date closed	Status	Category	N/C or C/I #	Client name

Compliance Audit Form (Verbal Disputes)				
Collector:		Supervisor:		
Account Number	(Legal / Ethical / Professional)	Requirements Met (FDCPA, FCRA, HIPPA)	Resolution	Comments
Audit Completed By:		Date:		

Here is your “Gramm-Leach-Bliley Act Compliance Package”…

I would highly suggest you make a Master File by copying the entire file to a Readable/Writable CD before signing any of the documents.

Keep this master file in a save place to use in the future.

Read through all the documents as well as the instruction sheet prior to starting your final procedures.

The number of security officers will depend on the size of your operation as well as the depth of your security checks.

All Security Officers should read pages 33656 through 33659 o 16 CFR 313 (I have provided a hyperlink to the FTC GLBA web site… http://www.ftc.gov/privacy/glbact/glbsub1.htm ... so they have a clear understanding of the data they are charged with protecting.

There are some added forms used to comply with the FDCPA and for general usage.

If you have any questions do not hesitate to call me at 405-833-2327

Ron L. Brown

GLBA / FDCPA / FCRA COMPLIANCE
PACKET INSTRUCTION SHEET

GLBA Declaration of Compliance – To be signed by the person appointed as "Director of Information Security" and a copy provide to each client.

GLBA Employee Compliance Agreement – To be signed by each employee of your company, no exception. Copy 1 to Personnel File and Copy 2 to the employee.

GLBA Employee/Agent Agreement – To be signed by any outside vendors or agents used by your agency whom might have access to NPPI. Copy 1 to file, Copy 2 to the signor.

DUE DILIGENCE WITH PROTECTED INFORMATION – copy to every employee.

GLBA Information Security and Confidentiality Officer – To be completed and signed as indicated. Copy 1 to file, Copy 2 to ISCO, Copy 3 to Client.

GLBA Security Check Sheets (Administrative, Technical, Physical) – Complete as indicated, Copy 1 to file, Copy 2 to ISCO/s. Perform these checks on a 6 month schedule.

GLBA Federal Register Part III, 16 CFR Part 313 – Copy to file, Copy to each ISCO.

FDCPA – Personal Property Release Receipt – To be signed anytime a consumer pays money to the agency for any reason.

Notice of Intent – Used prior to lien title procedures Voluntary Surrender Receipt – Used when Consumer surrenders property.

The Gramm-Leach-Bliley Act and Your Responsibility to the Client

Numerous federal, state and local statues relate to the protection and safekeeping of information provided by consumers to financial institutions and other types of businesses who provide financing or engage in the practice of lending money. There are also overlapping statues which relate to personal health information, credit reporting agencies, third party debt collectors and recovery specialists when a financial institution provides personal information to these service providers.
Service providers are recognized as ***"Business Associates"*** and may have access to any personal information the financial institution has obtained from the consumer as is required for the **service provider** to perform it's requested task.
It is then the responsibility of the ***"Business Associates",*** its employees and agents to offer the same protection to the personal information supplied to it to perform the requested task as would be required of the original financial institution.
To ensure proper due diligence with the consumers information held by our agency, its employees, agents and vendors and to properly protect the integrity of our information security system GLBA information should be distributed to all employees, agents and vendors who in any way would have access to a consumers personal information.

GRAMM – LEACH – BLILEY ACT (GLBA)
This is a relatively new federal privacy regulation. The date for the "Final Rule" implementation was May 24, 2004 and the law has been in full effect since that date.
The GLBA imposes new obligation regarding disclosure of information sharing practices, but with limited exceptions does not bar the sharing of information with affiliates and business associates. GLBA extends these disclosure rules to a broader range of business firms and a broader range of information than the FCRA and FDCPA.
All requirements of the GLBA on covered businesses extended to any business associate who works for or with protected information.
It is important that we, as business associates, clearly understand the definition of certain terms as they apply to this statue.

"FINANCIAL INSTITUTION" is broadly defined to include any institutions, the business of which is engaging in financial activities. Apparently the definition encompasses "institutions" even if they are not affiliated with financial services, holding companies or bank holding companies, but are merely engaged in a listed activity which is "financial in nature".

"NONPUBLIC PERSONAL INFORMATION" means personally identifiable information provided by a consumer to a financial institution, resulting from any transaction between a financial institution and the consumer or otherwise obtained by a financial institution, but not publicly available information. In the "Final Rule" Non Public Personal Information (NPPI) is clarified as information that is not "official public record", "available through widely distributed media". and "information required to be disclosed by federal, state or local law". As is obvious the issues of clarification are endless.

Although some of this information might be defined as "Public Information" much of the information is "not publicly available" and it should your firm's policy that the list of NPPI that you develop should include but not be limited to the following:

Social Security Numbers
Dates of Birth

Telephone Numbers
Drivers License Numbers
Any Derogatory Information
Any Financial Information (original balances, payment amounts past due amounts, etc.)
Any account numbers relating to financial transactions (checking/savings/accounts, credit/debit cards, loan numbers)
Name of Relatives or References
Dated of Transactions
Addresses
Vehicle Information
Child Support Information
Income Information
Insurance Information
Employment Information
Health Information
Bankruptcy Information

When sending any of the above information to a consumer or their legal representative it shall always be your company's policy to require the request to be in writing and approved by management staff.

To ensure proper compliance with this act your agency should appoint a designated employee or employees as Information Security and Confidentiality Officer/s.

These designates shall be responsible for identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.

These designates shall design and implement safeguards to control the risks identified through risks assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

These designates should oversee all service providers to your agency by taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue and requiring the selected service providers, by contract, to implement and maintain such safeguards.

These designates shall evaluate and adjust the information security program in light of the results of the testing and monitoring requirements of this section, any material changes to the operations or business arrangements, or any other circumstances that is known or should be known which might have a material impact on the information security program.

These designates should read all of the above and sign a statement stating that they understand their responsibilities as Information and Security Officer/s and agree to fulfill those duties as are set forth.

GRAHAM-LEACH-BLILEY
EMPLOYEE COMPLIANCE AGREEMENT

Date____/____/_____

I hereby confirm that I have been trained in the requirements of the Graham-Leach-Bliley Act.

I understand the definition of "non-public personal information" and the restrictions related to the disclosure of any information given to me in the course of my employment.

I acknowledge that it is my responsibility to protect and guard any "non-public information given to me in the course of my employment with _____.

I acknowledge that any inadvertent or intentional violation of the GLBA will be reported to my immediate supervisor immediately after such occurrence might happen.

I acknowledge that any violation of company policy related to the protection of "non-public personal information may be cause for immediate termination.

Signature_____

Job Title_____

GLBA/HIPAA BUSINESS ASSOCIATE/EMPLOYEE AGREEMENT

AGREEMENT made this ___day of_____, 200__, between Action Recovery & Collections LLC, hereafter Business Associate and _____ hereafter Employee.

WHEREAS, Business associate performs recovery services for a covered Entity, as defined by the Gramm-Leach-Bliley Act it's Implementing Regulations, and HIPAA and it's implementing procedures subsection 160.103 and has entered into a Business Associate Agreement ("Agreement") permitting the use and disclosure of Non Public Personal Information (NPPI) and Protected Health Information (PHI); and

WHEREAS, the Agreement further provides circumstances under which the Business Associate may disclose to an employee, agent or subcontractor NPPI and/or PHI received or created, subject to the provisions and limitations imposed under the Acts,

NOW, THEREFORE, the parties hereto agree as follows:

1. **Employee may receive from the Business Associate NPPI/PHI only as necessary to perform its obligations to Business Associate and to be used only for the purpose for which it is disclosed to the Employee.**

2. **Employee agrees to maintain the confidentiality of the NPPI/PHI and to affirmatively notify Business Associate of any breach thereof.**

3. **Employee agrees to the same condition and conditions that apply to the Business Associate With respect to such NPPI/PHI.**

4. **Employee may disclose information if required or permitted by law.**

EMPLOYEE

(Action Recovery & Collections LLC)

GLBA EMPLOYEE/AGENT AGREEMENT FOR BUSINESS ASSOCIATES

AGREEMENT made this _____day of _____, 200__, between_____, hereafter Business Associate and _____, hereafter Employee/Agent.

WHEREAS, Business Associate performs certain recovery services for a covered Entity, as defined by the Gramm-Leach-Bliley Act and has entered into a Business Associate Agreement ("Agreement") permitting the use and disclosure of Non-Public Information (NPPI); and

WHEREAS, the Agreement further provides circumstance under which the Business Associate may disclose to an employee, agent or subcontractor NPPI received or created, subject to the provisions and limitations imposed under the Act.

NOW, THEREFORE, the parties hereto agree as follows:

1. **Employee/Agent may receive from the Business Associate NPPI only as necessary to perform its obligations to Business Associate and to be used only for the purpose for which it is disclosed to the Employee/ Agent.**

2. **Employee/Agent agrees to maintain the confidentiality of the NPPI and to affirmatively notify Business Associate of any breach thereof.**

3. **Employee/Agent agrees to the same condition and conditions that apply to the Business Associate with respect to such NPPI.**

4. **Employee/Agent may disclose information if required or permitted by law.**

_____
EMPLOYEE/AGENT

_____
DIRECTOR OF INFORMATION SECURITY

INFORMATION SECURITY AND CONFIDENTIALITY OFFICER

Date___/___/____

As of this date the following person/persons shall be designated as Information Security and Confidentiality Officer/s.

1.

2.

3.

These designates shall be responsible for identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.

These designates shall design and implement safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

These designates should oversee all service providers by taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue and requiring the selected service providers, by contract, to implement and maintain such safeguards.

These designates shall evaluate and adjust the information security program in light of the results of the testing and monitoring requirements of this section, any material changes to the operations or business arrangements, or any other circumstances that is known or should be known which might have a material impact on the information security program.

I have read all of the above understand my responsibilities as Information and Security Officer and agree to fulfill those duties as are set forth.

1.

2.

3.

SECURITY CHECK SHEET / INFORMATION SECURITY PROGRAM

Date___/___/____

Physical: This will include all areas of physical procedures, including but not limited to the physical security of data outside the office with field employees, supervision, monitoring, retrieval and storage of all printed data.

Employees in this area of operations:

Assessment:

Possible Breaches of Security:

Recommended Changes to Protect Information Security:

Response to Recommendations:

SECURITY CHECK SHEET / INFORMATION SECURITY PROGRAM

Date___/___/____

Administrative: This will include all areas of administrative procedures, including but not limited to receiving and inputting data from clients, production and distribution of data to other areas of the operations, retrieval of data once assignment has been closed, storage of data, billing and crediting to clients accounts.

Employees in this area of operations:

Assessment:

Possible Breaches of Security:

Recommended Changes to Protect Information Security:

Response to Recommendations:

SECURITY CHECK SHEET / INFORMATION SECURITY PROGRAM

Date___/___/____

Technical: This will include all areas of technical procedures, including but not limited to computer operations and maintenance and storage of data. Selection and supervision of policies of all outside vendors and sub-contractors:

Employees in this area of operations:

Assessment:

Possible Breaches of Security:

Recommended Changes to Protect Information Security:

Response to Recommendations:

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

The HIPAA rules set the “floor” for national privacy standards relating to ***personal health information.*** It shall be our firms policy to give no ***personal health information*** to anyone other than the patient or their legal representative and then only with a written request and management approval. It shall be the policy of our firm that any personal health information obtained through any source shall be protected until same can be returned to its owner or destroyed in an appropriate manner.

FAIR DEBT COLLECTIONS PRACTICES ACT (FDCPA)

The FDCPA is very clear as to the information which may or may not be given out to third parties. Our firm and all employees, when and if it is applicable, shall explicitly and with no exceptions follow all the requirements of section 804, Acquisition of Location Information, when skip tracing and the requirements of section 805, Communication In Connection With Debt Collection, when communicating with a consumer regarding a debt.

FAIR CREDIT REPORTING ACT (FCRA)

The Fair Credit Reporting Act lists the permissible purposes under which a party may pull Consumer Report from a Consumer Reporting Agency. The permissible purposes are listed in sub section 604 (15 USC 1681b) and our firm and its employees shall explicitly and with no exceptions follow all the requirements of The Fair Credit Reporting Act and any amendments relating to same.

VOLUNTARY SURRENDER RECEIPT

IT IS ACKNOWLEDGED THIS_____DAY OF_____200__ THAT:

YEAR_____MAKE_____MODEL_____

VIN_____, COVERED BY A DEFAULTED SECURITY

AGREEMENT HELD BY _____,

HAS BEEN VOLUNTARILY SURRENDERED BY_____,

TO_____ LEGAL AGENT ACTING ON BEHALF OF THE REGISTERED LIENHOLDER, PURSUANT TO THE UNIFORM COMMERCIAL CODE OF THE STATE OF_____.

SURRENDERED BY_____

RECEIVED BY_____

PROPERTY RELEASE RECEIPT

Date___/___/____

Property Description_____
_____

Relating to mortgaged vehicle_____

Lienholder_____

I _____ do

hereby acknowledge a direct indebtness in the amount of $_____._____

to _____, of _____related to

services and/or storage of the aforementioned property.

_____
Person Receiving Property

_____
Witness

NOTICE OF INTENT

Date___/___/____

Be advised, pursuant to the Statues of the state of _____ relating to stored, parked or abandoned vehicles; our firm will initiate process on ___/___/____ to obtain a title and sell at auction the following described property to satisfy storage and/or other outstanding charges.

Description of property:

Registered owner:

Legal Owner:

To protect your interest in this property the sum of $_____.____ in certified funds must be received by our firm no later than 12:00 noon on ___/___/____.

This will be our final notice prior to application for a Lien Title and additional costs of $250.00.

Attn: Lien Title Division

COMMUNICATION IN THE ERA OF CYBERSPACE

In today's world of cyber space communications the professional recovery specialist is faced with many challenges. The majority of the consumer protections laws, both state and federal, were written before any of these cyber space communication tools and web sites were even thought of and therefore are antiquated in application.

I am asked daily about communication via e-mail or voicemail and if there are laws which prohibit this type of communication. My answer is always the same, **"BE VERY CAREFULL AND ERR ON THE SIDE OF CAUTION".**

The advantages of using e-mail, instant messaging and social web sites such as ***MYSPACE*** and ***FACEBOOK*** are numerous and indisputable. In today's era of ***CYBERBABIES*** who only have cell phones, i-pods and computers we often find this is the only method of communication.

But where do we draw the line?

If your agency falls under the auspices of the Fair Debt Collection Practices Act there is the definite risk of third party disclosure and the use of false of misleading statements if you set up a bogus social site account.

If you do not fall under the **FDCPA** then you still have to contend with your state consumer protection law.

When I mention the state law to a lot of recovery specialist I get a blank stare, like duh…what law is that?

Every state has a consumer protection law and as a professional it is your obligation to know what this law says and avoid violations which might occur when using **CYBER SPACE COMMUNICATION TOOLS.**

If you choose to communicate with a consumer through e-mail then you must absolve or at least minimize your risk. This can be accomplished in several ways, (1) if you are able to obtain express consent and permission from the consumer to receive communications via e-mail. Many of the current credit applications now have a space and check off box for an e-mail address and permission to communicate via electronic communication methods. (2) a web site in your name with a check off box and (3) oral permission granted in person or telephonically.

If you choose to communicate via social sites be sure to remember that all those communications are subject to viewing by third parties and there must be so mention of an indebtness, pending legal action or pending repossession.

The methods of communication, cyber tracking and skip tracing are changing daily at a breakneck speed and if we, as **PROFESSIONAL RECOVERY SPECIALISTS,** must change and adapt accordingly in order to continue to operate our business in a profitable manner.

Ron Brown, IFCCE, MCE is available on a consulting basis for all matters related to FDCPA, FCRA, GLBA, TRPPA and RED FLAG Compliance. He may be contacted via e-mail at Rbrown2150@aol.com or telephonically at 405-833-2327.

FRAUD / IDENTITY THEFT
CLIENT NOTIFICATION FORM

Pursuant to 15 USC 1681m (g) of the FACT Act you are hereby notified of a claim of Fraud and/or Identity Theft related to this debt.

Date_____ Case #_____

Client_____

Address_____

Contact_____

Consumer_____

_____

Amount_____

Date Turned_____

Statement_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

This report generated by _____
Computer Notes Entered_____

CONSUMER DISPUTE INVESTIGATION

Client _____Case #_____

Consumer
_____

Date Listed _____M/Notification Date _____ Dispute Date _____

Specified Nature of Dispute:
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Date of Investigation_____
Investigated By_____

Client Response_____
_____
_____
_____
_____
_____

Back Up Documents_____
_____

Action Taken_____
_____
_____
_____
_____
_____

NOTIFICATION OF FINDINGS

Case #_____

Client_____ Consumer_____

In regards to your written dispute received by our office on ___/___/____.

Pursuant to the requirements of 15 USC 1681m (g) our firm has notified the abovementioned client that this is a disputed claim.

Our firm has conducted a reasonable investigation of your dispute as required by 15 USC 1681s-2(a) (8) and our finding and action taken are as follows:

Findings_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Action Taken
_____
_____
_____
_____
_____

Do not get "TRPPA'd" into sharing a cell with your Recovery Agent!

H.R. 4709, Telephone Records and Privacy Protection Act of 2006 (TRPPA) is now federal law and could be your one way ticket to a huge fine, imprisonment or both.

If you, the lender, use a Recovery Agent or Skip trace Company who violated the strict guidelines of this new law then it is possible that you and your lender institution could face enhanced fines as well as a term in a federal prison of up to 5 years.

This new law criminalizes and makes it a federal offence to use pretexting in order to obtain customer information form the telephone services providers or their customers. It also prohibits and criminalizes the sale and transfer of telephone call records without prior authorization of the customer.

Typical of government bills "confidential phone records" is not clearly defined, however from prior ruling it can be identified to include ID or Account Numbers, Phone Numbers, Addresses and Toll Call Records.

Many Skip tracing companies have used this type of information on the past and continue to use it in violation of this law to locate missing consumers and mortgaged property. The new law makes it very clear that if your or lending institution have knowledge of fraudulent statements being used to gain the information or if you have not used due diligence in selection your recovery agent or skip trace company then you and your entity will be held liable and subject to the same penalties as the person or company committing the overt act.

This law passed the House and Senate and has been signed into law by President George Bush. It is in time and to protect yourself and your lending institution you should ask your Recovery Agency for a "H.R. 4709, TRAPP Statement of compliance".

If you ask for this document and get a blank stare…
My advice would be that you better beware.

Ron L. Brown, IFCCE
Confidential Security Investigations
Oklahoma City, OK

ACTION RECOVERY & COLLECTIONS LLC.
425 SHAMBURGER LN.
LITTLE ROCK, AR. 72206

H.R. 4709
TELEPHONE RECORDS AND PRIVACY PROTECTION ACT OF 2006
EMPLOYEE COMPLIANCE AGREEMENT

Date___/___/___

I hereby confirm that I have been fully trained in all the requirements for compliance as related to H.R. 4709.

I understand the violation of any section of H.R. 4709 is a violation of federal law may result in a fine and/or imprisonment of up to 10 years

I acknowledge that it is my responsibility to operate and trace within the guidelines of H.R. 4709 and all other applicable federal, state and municipal statutes in the course of my employment with ACTION RECOVERY & COLLECTIONS LLC.

I acknowledge that any inadvertent or intentional violation of the H.R. 4709 will be reported to my immediate supervisor immediately after such occurrence might happen.

I acknowledge that any violation of company policy related to the adherence to the statutes and requirements of H.R. 4709 may be cause for immediate termination as well as civil and/or criminal litigation.

Signature _____

Job Title_____

ACTION RECOVERY & COLLECTIONS LLC
425 SHAMBURGER LN.
LITTLE ROCK, AR. 72206

GRAMM-LEACH-BLILEY ACT DECLARATION OF COMPLIANCE

Action Recovery & Collections LLC, its Employees and Agents do hereby agree to keep all nonpublic personal information (NPPI), as defined in 16 CFR 313.3(n), about a customer of any client, whether in paper, electronic, or other form, confidential and shall not make any unauthorized disclosure of such information.

Furthermore, Action Recovery & Collections LLC, its' Employees and Agents agree not to use such nonpublic personal information for any purpose other than what is reasonably necessary to fulfill the purpose for which information was provided by said client.

Furthermore in compliance with the requirements of 16 CFR 314.4, Action Recovery & Collections LLC, does hereby declare that a program has been developed and instituted to implement and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards to achieve the required goals of 314.4.

Director of Information Security

_____/_____/_____
Date

ACTION RECOVERY & COLLECTIONS LLC.
425 SHAMBURGER LN.
LITTLE ROCK, AR 72206

FDCPA
DECLARATION OF COMPLIANCE

Action Recovery & Collections LLC, its Employees and Agents do hereby agree to abide by all rules, requirements and regulations of FDCPA including but not limited to all required disclosures and protection of covered data.

Furthermore, Action Recovery & Collections LLC, its' Employees and Agents acknowledge that they fully understand the purpose and intent of FDCPA and agree follow the dictates to ensure compliance in all areas.

Furthermore in compliance with the requirements of FDCPA, Action Recovery & Collections LLC does hereby declare that a program has been developed and instituted to implement and maintain a comprehensive Monitoring program that contains administrative, technical, and physical safeguards and programs to achieve the required goals FDCPA.

Director of Compliance and Security

_____/_____/_____
Date

ACTION RECOVERY & COLLECTIONS
425 SHAMBURGER LN.
LITTLE ROCK, AR. 72206

FCRA
DECLARATION OF COMPLIANCE

Action Recovery & Collections LLC, its Employees and Agents do hereby agree to abide by all rules, requirements and regulations of FCRA including but not limited to all required disclosures and protection of covered data.

Furthermore, Action Recovery & Collections LLC, its' Employees and Agents acknowledge that they fully understand the purpose and intent of FCRA and agree follow the dictates to ensure compliance in all areas.

Furthermore in compliance with the requirements of FCRA Action Recovery & Collections LLC. does hereby declare that a program has been developed and instituted to implement and maintain a comprehensive Monitoring program that contains administrative, technical, and physical safeguards and programs to achieve the required goals FCRA.

Director of Compliance and Security

_____/_____/_____
Date

ACTION RECOVERY & COLLECTION LLC
425 SHAMBURGER LN.
LITTLE ROCK, AR. 72206

FACTA
DECLARATION OF COMPLIANCE

Action Recovery & Collections LLC, its Employees and Agents do hereby agree to abide by all rules, requirements and regulations of FACTA including but not limited to all required disclosures and protection of covered data.

Furthermore, Action Recovery & Collections LLC, its' Employees and Agents acknowledge that they fully understand the purpose and intent of FACTA and agree follow the dictates to ensure compliance in all areas.

Furthermore in compliance with the requirements of FACTA, Action Recovery & Collections LLC does hereby declare that a program has been developed and instituted to implement and maintain a comprehensive Monitoring program that contains administrative, technical, and physical safeguards and programs to achieve the required goals FACTA.

_____
Director of Compliance and Security

_____/_____/_____
Date

Action Recovery & Collections LLC
425 Shamburger LN.
Little Rock, AR 72206

HIPAA
DECLARATION OF COMPLIANCE

Action Recovery & Collections LLC, its Employees and Agents do hereby agree to abide by all rules, requirements and regulations of HIPPA including but not limited to all required disclosures and protection of covered data.

Furthermore, Action Recovery & Collections LLC, its' Employees and Agents acknowledge that they fully understand the purpose and intent of HIPPA and agree follow the dictates to ensure compliance in all areas.

Furthermore in compliance with the requirements of HIPPA, Action Recovery & Collections LLC does hereby declare that a program has been developed and instituted to implement and maintain a comprehensive Monitoring program that contains administrative, technical, and physical safeguards and programs to achieve the required goals HIPPA.

_____

Director of Compliance and Security

_____/_____/_____
Date

ACTION RECOVERY & COLLECTIONS LLC
425 SHAMBURGER LN.
LITTLE ROCK, AR. 72206

TCPA
DECLARATION OF COMPLIANCE

Action Recovery & Collections LLC, its Employees and Agents do hereby agree to abide by all rules, requirements and regulations of TCPA including but not limited to all required disclosures and protection of covered data.

Furthermore, Action Recovery & Collections LLC, its' Employees and Agents acknowledge that they fully understand the purpose and intent TCPA and agree follow the dictates to ensure compliance in all areas.

Furthermore in compliance with the requirements TCPA, and Action Recovery & Collections LLC does hereby declare that a program has been developed and instituted to implement and maintain a comprehensive Monitoring program that contains administrative, technical, and physical safeguards and programs to achieve the required goals TCPA.

_____
Director of Compliance and Security

_____/_____/_____
Date

ACTION RECOVERY & COLLECTIONS LLC
425 SHAMBURGER LN.
LITTLE ROCK, AR. 72206

TRPPA
DECLARATION OF COMPLIANCE

Action Recovery & Collection LLC, its Employees and Agents do hereby agree to abide by all rules, requirements and regulations of TRPPA including but not limited to all required disclosures and protection of covered data.

Furthermore, Action Recovery & Collections LLC, its' Employees and Agents acknowledge that they fully understand the purpose and intent of TRPPA and agree follow the dictates to ensure compliance in all areas.

Furthermore in compliance with the requirements of TRPPA, Action Recovery & Collections LLC9 does hereby declare that a program has been developed and instituted to implement and maintain a comprehensive Monitoring program that contains administrative, technical, and physical safeguards and programs to achieve the required goals TRPPA.

_____

Director of Compliance and Security

_____/_____/_____
Date

THIS PAGE LEFT BLANK INTENTIONALLY