

PROPOSED PROCEDURES FOR AN IDENTITY THEFT PROTECTION PROGRAM

Setoff Debt Collection and GEAR Collection Programs

The Identity Theft and Fraud Protection Act (Act No. 190) allows for the collection, use and release of social security numbers to collect a debt, including a debt collected pursuant to the Setoff Debt Collection Act, Section 12-56-10, and the Governmental Enterprise Accounts Receivable Collections program, Section 12-4-580. SCAC has established internal procedures within the debt collection programs to further protect social security numbers and any other sensitive information to comply with Act No. 190 and the Federal Red Flag Rules.

The SCAC Identity Theft Prevention Program includes procedures to:

1. Identity red flags.
2. Detect red flags.
3. Respond to red flags.
4. Eliminate risk factors.
5. Minimize instances of identity theft.
6. Update the program, as necessary.

IDENTIFICATION OF RED FLAGS

This listing includes potential areas of interest that should be considered when identifying “red flags” for the Setoff Debt and GEAR programs. It may not be an exhaustive list for your entity given any unique types and/or amount of activity in handling and managing information that includes Personal Identifying Information (PII) such as Social Security Numbers (SSN), drivers license numbers, medical information, criminal records, financial information and more.

- Actual notices of identity theft from SCAC, entities, and/or SCDOR.
- Notices from SCDOR and/or entities that SSN and Name do not match
- Data from entities showing different names for same SSN
- Error Report from SCDOR for an SSN showing name submitted in program does not match name on tax return.
- No certification from entities discussing due process for debtors; accuracy of data; and compliance with identity theft policies
- Lost files containing Personal Identifying Information (PII)
- Emails containing PII sent to wrong addresses or intercepted by unauthorized individuals.
- Mail containing PII sent to wrong address
- Computers with PII that are left on and accessible to unauthorized individuals.
- Laptops containing PII lost, stolen, or left unattended
- Files and/or information, reports, documents with PII left on desks and accessible by unauthorized individuals
- Files and/or information, reports, documents that cannot be accounted for and may be lost or stolen
- Releasing PII to an unauthorized individual via telephone
- File Cabinets/Storage Rooms containing PII that are accessible to unauthorized individuals
- Keeping more files with PII than necessary.
- Lack of training for staff who handles PII.
- Lack of proper supervision for staff who handles PII

DETECTION OF RED FLAGS

Compliance for detecting red flags may need to focus on two areas of practical application- standards for the security of Personal Identifying Information, and standards for internal security.

Standards for Securing Personal Identifying Information

- Specifically defining access to data by employees;
- Defining procedures for the chain of custody of data;
- Insuring that the data, to the best of your knowledge and belief, is true, correct, and complete.
- Complying with due process and identity theft requirements;
- Managing and containing who is eligible to receive data;
- Defining procedures to respond to requests to disclose protected health information;
- Developing policies and procedures for safeguarding sensitive information, such as locked file cabinets; key access to rooms; secure workstations; data control, and more.
- Defining staff procedures for transmitting data through electronic transfer; email; fax; and mail;
- Defining procedures for retaining detailed match records and any other reports containing PII;
- Defining procedures for handling notices of actual and/or potential identity theft;
- Providing appropriate training to staff who handle PII; and
- Providing appropriate supervision of staff and documents/files/reports.

Standards for Internal Security

- Developing password policies to protect data;
- Complying with approved InfoSec guidelines for operating system configuration
- Protecting access to areas containing sensitive information.
- Insuring that most recent security patches are installed on computers.
- Locating servers in an access-controlled room.
- Defining server and work-station security, including virus protection policies;
- Defining security strategies for email and internet usage;
- Developing policies for transferring data;
- Using standard security principles of least required access to perform a function; and
- Installing firewalls that are configured to allow communications over set protocols between defined machines.

RESPONDING TO RED FLAGS/ ELIMINATING RISK /MINIMIZING IDENTITY THEFT

The response to red flags will require additional policies and/or procedures for mitigating potential identity theft by identifying the risk and taking any necessary corrective actions. Responses may include upgrades in virus protection; firewall enhancements; locking mechanisms and access control for rooms, file cabinets, computer workstations, laptops, etc.; password protection; staff training on handling PII; fax security; secure socket layer transmission software (already established by SCAC for Setoff Debt and GEAR programs); controls for custody of data; verifying SSNs when notified of potential errors; establish appropriate supervision for staff handling PII; and disposing unnecessary information containing PII to include hard-copy documents and electronic files/documents. *This is not an exhaustive list. Your entity may need additional policies and/or procedures given any unique types and/or amount of activity in handling and managing PII information.*

Managing Identity Theft Notifications

When SCAC receives a notification from an entity or SCDOR that a SSN is suspected or verified to be a case of identity theft, SCAC will immediately share this information with all other affected entities, SCDOR, and Five Star. The account will be zeroed in SCAC's system and an adjustment will be sent to SCDOR in the next adjustment file submission. Entities will be notified in writing about the actual/suspected identity theft with the recommendation to share the information with their attorney and take appropriate action. Any account identified as an actual case of identity theft will be red-flagged in the SCAC system. Any future submissions of this account by entities with the same SSN and name will be zeroed and the entities will be notified of the identity theft.

Any information from SCDOR's Tax System that shows a SSN and Name do not match information in our system will be forwarded to the appropriate entities. SCAC will share this information and recommend that the entity reviews the data and submits the appropriate adjustment to SCAC, as necessary. Also, SCAC will take similar action for any error report from SCDOR following a match showing that the name submitted to the Setoff Debt and/or GEAR programs with a SSN does not match the name on a tax return. This information will be provided to the appropriate entity and SCAC will request the entity to review the data and make appropriate adjustments to the account(s).

In instances where more than one entity has submitted the same SSN with different names, SCAC will notify the affected entities and request a review of accounts. If the entity discovers an error or cannot verify the name and SSN for an individual, SCAC will request that the entity notify SCAC and submit an adjustment file that zeros the account.

Responding to Breaches

A breach of the Red Flag Rules means an incident of unauthorized access to and acquisition of records or data that discloses Personal Identifying Information outside of the organization that compromises the security, confidentiality, or integrity of PII and could be used for illegal purposes to harm an individual. It does not include incidents such as an unauthorized staff member seeing a setoff debt report on the desk or computer monitor. If a breach has occurred with an individual's debt record, the incident should be documented, identifying the nature of the breach. The incident should be reported to your internal Compliance Committee and appropriate action should be taken to notify the individual and to insure this type of breach does not reoccur.

MONITORING AND UPDATING THE IDENTITY THEFT PREVENTION PROGRAM

Entities should monitor the program and report to your internal Compliance Committee any concerns or questions about securing PII. The program should be modified to address these concerns, as necessary.

Checklist for Establishing an Identity Theft Prevention Program Setoff Debt and GEAR Collection Programs

Take Stock: Know what personal information you have in your files and on your computers.

- What type of sensitive information do you collect and/or maintain ?
(i.e. SSN, name, debt data, bankruptcy information, address changes, payments, protests, inquiries for data, certification of hearings, deceased notifications, wrong SSN notifications, identity theft notifications, banking information, and more)
- Where do you store sensitive data ? *(rooms? file cabinets? computers?)*
- Who has access to your data ? *(chain of custody)*
- How is data transferred to you internally and by outside agencies/organizations ?
(i.e. Setoff Debt and/or GEAR information is electronically transferred to and from SCAC using Secure Socket Layer (SSL) technology through a website and/or SCAC debt software.)
- How do you transfer sensitive data to other employees, offices, outside service providers ?
(via secure website; secure email; mail; fax)
- Do you create PII records internally ? *(Computer files, phone records, reports, post-it notes)*
- How do you acquire PII necessary to submit accounts to Setoff Debt and/or GEAR ? How is this data stored and managed upon collection ?

Scale Down: Keep only what you need for your business

- How do you use SSNs and other sensitive data ? *(SSNs are required data fields for submitting debts. When printing letters/reports/documents/analyses, do you need the full SSN ? Or, can you use the last 4 digits ?)*
- Do you include PII in unencrypted emails ? *(remove sensitive information from emails)*
- What is your retention policy for keeping reports/documents/data files ?
- Do you keep credit card information ? Is there a need for this type of data ?
- Does everyone receiving data with PII need it ?
- Is it necessary for staff to create documents/notes/records/phone messages with PII ?
- Do you keep any unnecessary data that is not pertinent to the function of your office function ?
- Do you keep emails ? Archive procedures ? Deletion of unnecessary emails consistent with document retention and state/federal requirements ?
- How do you document phone conversations ? Do you keep records from phone calls with PII ? Is this data retained or destroyed ?
- Do you print and keep detailed reports from setoff matches or GEAR collections ? How long ?
- Do you keep returned mail from notifications that includes PII ? How are they stored ? Who has access to them ? Do you create any file or manifest to document the returned mail ? Or, do you actually keep the hard copies ? How do you dispose of the mail ?
- How long do you store the bankruptcy notices/ wrong SSN notices/ Deceased notices sent by SCAC ?

Lock It: Protect the information that you keep

- Is PII data/records/reports kept in a locked room or file cabinet ?
- Are all files containing PII put away in a secure location when not in use ?
- Are staff logging off computer applications; turning off monitors; and preventing others from accessing data on computers when not in office ?
- Does the building and/or office have secure access controls ?
- Is data encrypted if electronically sent over the internet ? *SCAC uses SSL technology to allow*

entities to send and receive data. SCAC will not use any unencrypted means, such as email, to transfer or receive data.

- Do you regularly update anti-virus and anti-spyware programs on individual computers ?
- Do you use more complex or smart passwords ? *Smart passwords are automatically built into the SCAC Debt Software and Web browser transfer applications.*
- Does the “Administrator” for the SCAC software properly maintain access controls for other staff to protect against unauthorized viewing of the data or changing data ?
- Are employees trained not to send PII data in unencrypted emails ?
- Do you have appropriate laptop security ?
- Do you have an adequate firewall to prevent unauthorized access to your network ?
- Do you have adequate access controls to only allow authorized staff to view files ?
- Are you monitoring incoming internet traffic for signs of breaches ?
- Do you check references and conduct background checks when hiring employees ?
- Do you have an appropriate procedure to remove individual’s access to data when he/she leaves your organization ?
- Does your employee training include computer security to avoid downloading harmful files from email and the internet ?

Pitch It: Properly dispose of what you no longer need.

- Do you have record disposal procedures in place ?
- Do you shred, burn sensitive documents containing PII ?
- Are shredders easily available to your staff ?
- Do you use wipe utility programs when disposing of old computers ?
- Do you have protection procedures for hard copy documents and records, laptops, electronic files that are provided to employees who are away from the office ?
- Once shredded, do you have appropriate backup procedures to find data to respond to debtor inquiries about accounts/collections/notifications/protests/possible errors ? (*SCAC maintains data files on all historical collections.*)

Plan Ahead: Create a plan for responding to problems/security incidents

- How do you handle notices sent by SCAC about possible identity theft ? SSN and name mismatch ? Error report showing problem with SSN ?
- Do you review and correct data based on error reports sent by SCAC ? *SCAC sends verification reports for every file received and includes error reports of problem accounts.*
- Do you review and make any necessary corrections to inventory reports and reconciliation reports sent by SCAC ?
- How do you respond to security incidents ? Have you established a Compliance Committee ?
- How will you investigate security incidents ?
- Who do you notify about a security breach ? internal staff ? individuals outside office ?
- Do you have procedures to handle a compromised computer/laptop/server ?