

## ATTACHMENT II

### EXHIBIT 3

#### IRC SEC. 7213 UNAUTHORIZED DISCLOSURE OF INFORMATION.

##### (a) RETURNS AND RETURN INFORMATION.-

- (1) FEDERAL EMPLOYEES AND OTHER PERSONS. - It shall be unlawful for any officer or employee of the United States or any person described in section 6103(n) (or an officer or employee of any such person), or any former officer or employee, willfully to disclose to any person, except as authorized in this title, any return or return information [as defined in section 6103(b)]. Any violation of this paragraph shall be a felony punishable upon conviction by a fine in any amount not exceeding \$5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution, and if such offense is committed by any officer or employee of the United States, he shall, in addition to any other punishment, be dismissed from office or discharged from employment upon conviction for such offense.
- (2) STATE AND OTHER EMPLOYEES. - It shall be unlawful for any person [not described in paragraph (1)] willfully to disclose to any person, except as authorized in this title, any return or return information [as defined in section 6103(b)] acquired by him or another person under subsection (d), (i)(3)(B)(i), (1)(6), (7), (8), (9), (10), (12), (15) or (16) or (m)(2), (4), (5), (6), or (7) of Section 6103. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding \$5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.
- (3) OTHER PERSONS. - It shall be unlawful for any person to whom any return or return information [as defined in section 6103(b)] is disclosed in a manner unauthorized by this title thereafter willfully to print or publish in any manner not provided by law any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding \$5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.
- (4) SOLICITATION. - It shall be unlawful for any person willfully to offer any item of material value in exchange for any return or return information [as defined in 6103(b)] and to receive as a result of such solicitation any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding \$5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.
- (5) SHAREHOLDERS. - It shall be unlawful for any person to whom return or return information [as defined in 6103(b) ] is disclosed pursuant to the provisions of 6103(e)(1)(D)(iii) willfully to disclose such return or return information in any manner not provided by law. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding \$5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

**SEC. 7213A. UNAUTHORIZED INSPECTION OF RETURNS OR RETURN INFORMATION**

- (a) PROHIBITIONS. -
  - (1) FEDERAL EMPLOYEES AND OTHER PERSONS. -It shall be unlawful for-
    - (A) any officer or employee of the United States, or
    - (B) any person described in section 6103(n) or an officer willfully to inspect, except as authorized in this title, any return or return information.
  - (2) STATE AND OTHER EMPLOYEES. - It shall be unlawful for any person [not described in paragraph (1)] willfully to inspect, except as authorized by this title, any return information acquired by such person or another person under a provision of section 6103 referred to in section 7213(a)(2).
- (b) PENALTY. “-
  - (1) IN GENERAL. - Any violation of subsection (a) shall be punishable upon conviction by a fine in any amount not exceeding \$ 1000, or imprisonment of not more than 1 year, or both, together with the costs of prosecution.
  - (2) FEDERAL OFFICERS OR EMPLOYEES. - An officer or employee of the United States who is convicted of any violation of subsection (a) shall, in addition to any other punishment, be dismissed from office or discharged from employment.
- (c) DEFINITIONS. - For purposes of this section, the terms “inspect”, “return”, and “return information” have respective meanings given such terms by section 6103(b).

## **EXHIBIT 4**

### **IRC SEC. 7431 CIVIL DAMAGES FOR UNAUTHORIZED DISCLOSURE OF RETURNS AND RETURN INFORMATION.**

- (a) IN GENERAL. -
- (1) INSPECTION OR DISCLOSURE BY EMPLOYEE OF UNITED STATES. - If any officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against the United States in a district court of the United States.
- (2) INSPECTION OR DISCLOSURE BY A PERSON WHO IS NOT AN EMPLOYEE OF UNITED STATES. - If any person who is not an officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against such person in a district court of the United States.
- (b) EXCEPTIONS. -No liability shall arise under this section with respect to any inspection or disclosure
- (1) which results from good faith, but erroneous, interpretation of section 6103, or
- (2) which is requested by the taxpayer.
- (c) DAMAGES. - In any action brought under subsection (a), upon a finding of liability on the part of the defendant, the defendant shall be liable to the plaintiff in an amount equal to the sum of-
- (1) the greater of-
- (A) \$ 1,000 for each act of unauthorized inspection or disclosure of a return or return information with respect to which such defendant is found liable, or
- (B) the sum of-
- (i) the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure, plus
- (ii) in the case of a willful inspection or disclosure or an inspection or disclosure which is the result of gross negligence, punitive damages, plus
- (2) the cost of the action.

- (d) PERIOD FOR BRINGING ACTION. - Notwithstanding any other provision of law, an action to enforce any liability created under this section may be brought, without regard to the amount in controversy, at any time within 2 years after the date of discovery by the plaintiff of the unauthorized inspection or disclosure.
- (e) NOTIFICATION OF UNLAWFUL INSPECTION AND DISCLOSURE. - If any person is criminally charged by indictment or information with inspection or disclosure of a taxpayer's return or return information in violation of-
  - (1) paragraph (1) or (2) of section 7213(a),
  - (2) section 7213A(a), or
  - (3) subparagraph (B) of section 1030(a)(2) of title 18, United States Code, the Secretary shall notify such taxpayer as soon as practicable of such inspection or disclosure.
- (f) DEFINITIONS. - For purposes of this section, the terms "inspect", "inspection", return" and "return information" have the respective meanings given such terms by section 6103(b).
- (g) EXTENSION TO INFORMATION OBTAINED UNDER SECTION 3406. - For purposes of this section-
  - (1) any information obtained under section 3406 (including information with respect to any payee certification failure under subsection (d) thereof) shall be treated as return information, and
  - (2) any inspection or use of such information other than for purposes of meeting any requirement under section 3406 or (subject to the safeguards set forth in 6103) for purposes permitted under section 6103 shall be treated as a violation of section 6103.

For purposes of subsection (b), the reference to section 6103 shall be treated as including a reference to section 3406.

## **10801.500 POLICY ON DISCLOSURE AND CONFIDENTIALITY OF INFORMATION**

**CITATIONS:** 42 U.S.C. 1320b-7; Section 6103 (1) (7) of the Internal Revenue Code; P.L. 93-579, The Privacy Act of 1974.

### **POLICY**

**1. Disclosure** BENDEX data is disclosed under the routine use rule and without the consent of the individual, provided the request is for a purpose which is compatible with the purpose for which it was collected.

SSA may also generally disclose information with the written consent of the individual. You should be familiar with these policies to assure that personal information is protected and disclosed when appropriate.

**2. Personal Information** SSA only discloses personal information when required by Federal law and does not disclose information when it is prohibited by Federal law.

**3. Disclosure Without Consent**

a. SSA may disclose benefit information to State welfare departments upon their request for use in determining a recipient's eligibility to WFFA, food stamps, Medicaid, or other income and health maintenance programs that are administered by the State.

b. SSA may disclose tax return information for administering these programs:

- WFFA
- Medicaid
- Food Stamps
- Unemployment Composition
- Child Support Enforcement

SSA may not disclose tax return information to states for other purposes.

- c. For Guam, Puerto Rico and the U.S. Virgin Islands, you may request earnings information for the programs named in b. above for any State program under title I, X, XVI of the Social Security Act.
  - d. If a program is not specifically listed, the State must request approval from SSA before using the data for the program.
- 4. Accounting For Disclosures**
- a. The State must keep a record for any redisclosure of MBR data to non-State entities who are not acting as agents of the State.
  - b. Redisclosure to another component within the State does not require accounting.
- 5. Independent Contractors**
- a. An independent contractor acting as an agent of the State is subject to IRS Safeguard Reviews. The contractor must establish written safeguard procedures describing the security measures to be taken to protect the Federal tax data.
  - b. The State agency must make periodic inspections of the facility and keep a written record of such inspections.
- 6. Disclosure With Consent**
- a. The individual must authorize the release of personal information requested for a nonprogram use.
  - b. The consent statement may be part of an application for social services, for example, or be on a separate paper. The State must retain consent statements for 2 years.

**10801.510 STANDARDS FOR PHYSICAL SAFEGUARD OF BENDEX AND BEER INFORMATION**

**A. POLICY**

**1. Physical Safeguards**

Physical safeguards are measures observed to:

- maintain confidentiality of personal information
- control access to personal data records
- protect personnel, equipment, records and facilities from accidents, hazards or disasters

This policy assures that there is limited access to BENDEX information provided by SSA.

**2. Spot Checks**

Management at all levels must perform adequate reviews and spot checks of daily activities to identify potential problems and to determine how well employees are adhering to the standards. Each office shall have a security officer and alternate appointed from the management staff.

**3. Contingency Plan**

The State central office must have a contingency plan for backup operations in case normal operations are disrupted.

**4. Disaster Plan**

Central and local offices must have a disaster plan to adequately provide for the protection of personnel, facilities, records and equipment in the event of natural or man-made disasters. The plan should be reinforced with training and drills.

**5. Security Officer**

The State Security Officer shall:

- Develop a security program based on the requirements of the Privacy Act, State standards and Federal government guidelines;
- Insure that each office maintains an adequate security action plan;
- Review and monitor the methods used to move BENDEX data with the agency and between the State and SSA;

- Be the primary point of contact with the SSA System Security Officer and provide support to the SSA System Security Officer when periodic reviews are conducted;
- Conduct training on all phases of security affecting the State office and its operations;
- Ensure that all instructions and procedures dealing with systems security are safeguarded; and
- Develop a checklist for conducting self-evaluation reviews.

#### **6. Audits**

Security audits should be conducted at least annually to sustain employee knowledge of the standards and what is expected of them in performing their duties.

#### **7. Reports**

An annual compliance report of the reviews conducted will be provided to the SSARO.

### **B. REFERENCES**

The State Income and Eligibility Verification (IEVS) Data Exchange Agreement;

IRS Pub. 1075, Tax Information Security Guidelines for Federal, State and Local Agencies.