In the matter of Arbitration between . . . . . .

AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES
AFL-CIO, LOCAL 3696

AND

FEDERAL BUREAU OF PRISONS
FCC BUTNER

RE: FMCS FILE NO. 13-53859-3

BUTNER, NORTH CAROLINA, DECEMBER 18, 2014

BRIEFS FILED: March 13, 2015

REPLY BRIEFS FILED: March 27, 2015

ARBITRATOR: Linda S. Byars

APPEARANCES:

For the Union

Stephanie J. Bryant, Mehri & Skalet, PLLC
Taryn Wilgus Null, Mehri & Skalet, PLLC

For the Employer

Michael Markiewicz, U.S. Department of Justice

BACKGROUND

The Federal Correctional Center, Butner, North Carolina, herein referred to as FCC Butner or the Agency, is part of the Department of Justice, Bureau of Prisons. There are three local unions representing the bargaining unit at FCC Butner. The American Federation of Government Employees, Local 3696, herein referred to as the Union, filed the Grievance on behalf of a class of employees protesting a Privacy Act violation.

By memorandum dated October 11, 2012 and signed by Acting Complex Warden Angela Dunbar, FCC Warden Gerri Levister, and FCC Warden Justin Andrews, all FCC Butner staff received notification of a security incident at FCC Butner. [Union Exhibit No.2.] The memorandum includes the following statements and recommendations that staff protect themselves from the possibility of identity theft:

> Today, we have been made aware that personally identifiable information (PII) of staff members within the complex may have been compromised. Some examples include: full name, address, social security number, date of birth and various account numbers. This information was discovered inside the safety recycling building as camp inmates were shredding the material. We have no evidence that any inmate has retained any of this information. However, we are taking steps to investigate the incident and to notify staff of ways to protect themselves. [Union Exhibit No. 2.]

By memorandum dated October 12, 2012, the Wardens notified the staff with an update on the security incident stating in relevant part the following:

> This evening, October 12, 2012, at approximately, 6:20 p.m. staff received additional information that confirmed an inmate who was assigned to the safety recycling building detail attempted to mail out paperwork with sensitive material, which included personally identifiable information (PII) of all staff members who were assigned to the complex on June 11, 2012. This material included full names, titles, pay-grades, enter on duty (EOD) dates, Social Security Numbers, and home telephone numbers. The sensitive material was intercepted by staff prior to it being mailed from the institution. The Federal Bureau of Investigations (FBI) has been

> notified and the investigation into this matter is on-going. [Union Exhibit No. 3.]

The October 12, 2012 memorandum reiterates the need for employees to protect themselves from identity theft and includes recommendations for doing so. [Union Exhibit No. 3.]

In an undated memorandum from Complex Warden Craig Apker and Wardens Dunbar, Andrews and Levister, the FCC Butner staff received notification that, "After an initial assessment and as a precaution, we are setting up a two-year credit monitoring service in your name at no cost to you." [Union Exhibit No. 5.][1] In another undated memorandum, Wardens Apker, Dunbar, Andrews, and Levister responded to inquiries concerning the possibility that the recovered documents contained staff family members' personal identifiable information, stating as follow:

> To date, we have identified one document that contains personal identifiable information of a staff's family member. That staff member has been contacted directly and was given an extra Equifax Promotion Code to accommodate their family member.[Union Exhibit No. 6.]

By Formal Grievance Form signed by Local Union President Ricky Arrington, on behalf of Local 3696, the Union alleges a continuing violation beginning October 11, 2012 of the parties' Master Agreement, the Freedom of Information and the Privacy Acts, describing the violation as follows:

> On October 11, 2012, the Union was notified by management that a staff member making rounds inside the Safety Recycling Center noticed inmates shredding files. The files contained personally identifiable information (PII) of staff member's full names, addresses, social security numbers, dates of birth & various account numbers.
>
> On October 12, 2012, the Acting Complex Warden, Angela Dunbar, generated a memorandum acknowledging that personal identifiable information had been confirmed to be in the possession of an inmate who

[1] The parties agree that the memo was distributed on October 22, 2012. [Transcript p. 110.]

was assigned to the safety recycling building detail and had attempted to mail out paperwork with sensitive material, which included personally identifiable information (PII) of all staff members who were assigned to the complex on June 11, 2012. The material included full names, titles, and pays grades, enter on duty (EOD) dates, social security numbers and home telephone numbers.

It is noteworthy that in the language of both Acting Warden Dunbar's memorandums to staff was informed that the matter was under investigation by several investigative entities. [Joint Exhibit No. 2.]

The Grievance requests the following remedy:

All attorney, legal fees and expenses incurred in the processing this grievance will be reimbursed by the agency. The grievant will suffer no reprisal, harassment, or intimidation, as a result of filling this grievance. Those suitable compensations are granted and any other remedy the arbitrator deems appropriate to make the Bargaining Unit employees whole. That the agency be ordered to pay the total cost of arbitration show (sic) this issue proceeds to arbitration based on a prohibited personal practice committed by the agency.

1) The Agency provides Local 3696 any and all uncensored investigative reports by any parties involved in reviewing/investigation this matter (no reacted (sic) information).

2) The Agency provide a copy of every document found pertaining to the release of possible sensitive information to each affected member of the Bargaining Class.

3) The Agency provide all staff members affected of the Bargaining Unit currently or formally employed at FCC-Butner with credit identify theft protection for life (Life Lock).

4) The Agency provide a letter of apology for every Bargaining member from the Mid-Atlantic Regional Director, Ike Eichenlaub, for the Agency's failure to notify the affected staff of the sensitive security breach in a timely manner. Additionally, with language to include, the Agency accepting accountability and responsibility for failure to safeguard staff sensitive information.

5) The Agency compensate each affected staff member employed at FCC Butner from January 2000 to the present a sum $300,000.00 for any possible past, present or future theft of identity or damages to their credit rating or those of their immediate family members.

6) Ship/rotate all current inmates from FCC Camp to Institutions outside the Region

7) Demote all supervisory staff connected to non-supervisory position.

1a. Insurance for spouses. [Joint Exhibit No. 2.][2]

By letter dated March 8, 2013, Warden Andrews responded by restating the Grievance and responding as follows:

> In your grievance you acknowledge that staff were informed that the matter was under investigation by several entities. The October 12, 2012 memo disseminated by the Wardens states that the Federal Bureau of Investigation (FBI) was notified and there is an on-going investigation.
>
> In most cases, investigations relating to potential staff misconduct are the responsibility of the Office of Internal Affairs or delegated to the local investigative team. However, because the FBI has taken jurisdiction of the investigation into this incident, and the investigation is on-going, the agency is not authorized to release information at this time. If you seek additional information that you feel may be outside the scope of the investigation, you may contact the Office of General Counsel, Freedom of Information and Privacy Act Section.
>
> Any requests for public information about an individual or requests for documents that are not related to an individual can be submitted electronically. Requests for non-public information about individuals cannot be accepted electronically.
>
> If the request involves non-public information about an individual, it must be in writing with the original signature of the person the records are about. The signature needs to be notarized or signed under penalty of perjury and mailed to:
>
> Freedom of Information Act/Privacy Act Section
> Office of General Counsel
> Room 841 FBOP
> 320 1st St. NW
> Washington, D.C. 20534
>
> Although the series of events surrounding this matter is regrettable, the Executive Staff have worked collectively to devise a plan of action to properly and expeditiously address this vital issue. As you are aware,

[2] The Grievance is signed by a recipient and dated November 29, 2012.

> Management has taken swift and decisive action since the beginning of this episode, and takes our obligation to protect personally identifiable information (PII) very seriously. Upon management learning of the incident your grievance discusses, the Union Presidents were informed and input was solicited from all parties on the most advantageous way to move forward. Formal memorandums were prepared from the Wardens advising and updating staff on the security breach and alerting them to the potential risks involved with the exposure of personally identifiable information. On October 22, 2012, formal notification was addressed to all staff that a two-year credit monitoring service would be provided to all staff free of charge by Equifax Personal Solutions. The 3-in-1 monitoring plan provides the following benefits:
>
> - Daily credit monitoring of Equifax, Experian and Trans Union Credit files.
> - Unlimited copies of your Equifax credit report.
> - A 3-in-1 Credit report which provides credit history as reported by the three major credit reporting agencies
> - Identity theft insurance in the amount of $1,000,000 per consumer to cover injuries arising from an occurrence of identity theft.
>
> Based on a thorough review of the recorded documents, former employees that were identified as potentially being impacted by this incident will receive the same benefits listed above.
>
> The Agency's response to this incident was immediate, and precautionary measures have been swiftly implemented to protect those employees who may be impacted. Because the investigation into this matter is on-going, additional remediation measures may be necessary at some point in the future, and such measures will be addressed and considered as the situation develops. As such, your grievance is granted to the extent that the credit monitoring addresses your concerns. Your requests for other remedies are, however, denied. [Joint Exhibit No. 3.]

By memorandum dated March 19, 2013, the Union notified the Agency of its intent to pursue arbitration. [Joint Exhibit No. 4.] By memorandum dated July 3, 2013, the Union made a request for information regarding the investigation, outlining the information needed by the Union. [Joint Exhibit No. 5.] By memorandum dated July 15, 2013, the Agency responded to the request for information. [Joint Exhibit No. 6.]

In an undated document, the Union made a second request for information, outlining the information needed by the Union. [Joint Exhibit No. 7.] By memorandum dated October 31, 2014, the Agency responded as follows:

> This is in response to your request for information pursuant to Title 5 United States Code (USC), Section 7114 (b) (4), which was received on August 7, 2014. In this, you request the agency provide all documents that refer or relate to documents contained in the files sent to Safety Recycling on or before October 12, 2012. This included but was not limited to documents that were confirmed to be in possession of an inmate; and all documents that refer or relate to any investigation the Agency conducted into the disclosure described in the grievance filed on November 29, 2012.
>
> In response to your request, please be advised the Agency has been in contact with Banumathi Rangarajan, Assistant United States Attorney, regarding release of this information to you. The Agency has been informed that this case is being investigated by the United States Attorney's Office and the Agency has been instructed not to release information pertaining to this case until the criminal investigation has been completed. Once the Agency receives notice from the United States Attorney's Office the criminal investigation has been completed, the Agency will revisit your data request. If you require additional assistance with this issue, please feel free to contact me. [Joint Exhibit No. 8.]

By memorandum dated December 1, 2014, the Agency again responded to the Union's information request, denying an obligation to provide requested information, but "in the spirit of cooperation" providing a response to the Union's information request. [Joint Exhibit No. 9.] Rather than postponing arbitration indefinitely, the Union decided to go forward with the Grievance while reserving its right to receive all of the investigative documents before proceeding with the damages portion of the case.

The Grievance came before the Arbitrator at hearing on December 18, 2014 in Butner, North Carolina. The parties entered the following stipulations:

1. Documents that were being shredded by an inmate work detail as referenced in the October 11th, 2012, memorandum for All FCC Butner Staff from Warden

Apker, Warden Dunbar, Warden Andrews and Warden Levister, included employee travel reimbursement vouchers, employee direct deposit forms, employee uniform allowance forms, institution credit card orders and invoices, and inmate commissary account documents. [Transcript p. 28.]

2. Documents that were contained in the paperwork that an inmate attempted to mail out of FCC Butner on October 12th, 2012, as referenced in the October 12th, 2012, memorandum for All FCC Butner Staff from Warden Dunbar and Warden Andrews, included handwritten pages of individual names, Social Security numbers, dates of birth of inmates and civilians. [Transcript p. 29.]
3. Employee travel reimbursement vouchers, employee direct deposit forms and employee uniform allowance forms are normally stored in a central file room for Accounting and Budgeting, Financial Management, LSCI, and filed by employee's last name. [Transcript p. 29.]

The parties submitted post-hearing briefs, received by the Arbitrator on March 13, 2015. The parties submitted reply briefs, received by the Arbitrator on March 27, 2015. The parties did not agree on a statement of issue; they frame the issues as follows. [Transcript pp. 11-12.]

STATEMENTS OF ISSUE

The Agency

Is the Grievance in the wrong jurisdiction? Is the Grievance timely? Did Management violate the Privacy Act in October of 2012, and if so what is the appropriate remedy?

The Union

Did the Bureau of Prisons, FCC Butner, violate the Privacy Act by disclosing FCC Butner employees' personal information to inmates in October 2012, and if so what is the remedy?

OPINION

Jurisdiction

The Agency first submits that the Grievance, alleging a violation of the Privacy Act, is outside the Arbitrator's jurisdiction. The Agency maintains that Congress intended the courts to have complete jurisdiction over alleged violations of the Privacy Act, as evident in its legislative history. The Agency contends that the Privacy Act statute was enacted to protect individual citizen rights in furtherance of Constitutional Rights and was not issued for the purpose of affecting working conditions or conditions of employment. The Agency further contends that the Federal Statute of the Privacy Act, unlike for example the Fair Labor Standards Act, specifically states that the district courts of the United States have jurisdiction. Contrary to the Agency's position, however, the Federal Labor Relations Authority has specifically found that alleged violations of the Privacy Act are grievable and that arbitrators have authority to decide such issues.

In *AFGE Local 987 and U.S. Department of the Air Force, Robins Air Force Base, Georgia*, 57 FLRA 551 (2001), the Authority concluded that, ". . . the Privacy Act is a law 'affecting conditions of employment' within the meaning of § 7103(b)(9)(C)(ii) of

the Statute." The Authority further concluded that, ". . . claimed violations of the Privacy Act come within the definition of 'grievance' set forth at § 7103(a)(9)(C)(ii), and are grievable and arbitrable under a broad-scope grievance procedure." The Authority also specifically held that, ". . . the damages provision of the Privacy Act is applicable to arbitration proceedings." The Authority again specifically rejected the Agency's jurisdiction argument in *U.S. Department of Veterans Affairs, Medical Center, Charleston, South Carolina and National Association of Government Employees*, 58 FLRA 706 (2003) and in *AFGE, Local 1045 and United States Department of Veterans Affairs Medical Center, Biloxi, Mississippi,* 64 FLRA 86 (2010). The case cited by the Agency as example of its position, *U. S. Customs Service v. FLRA*, 43 F.3d 682 (D.C. Cir. 1994) is not specific to the Privacy Act and is not on-point.

Citing, for example, *Parks v. IRS*, 618 F.2d 677 (10th Cir. 1980), the Agency also contends that Privacy Act rights are personal to the individual and cannot be asserted derivatively by others. However, unlike *Parks*, which was filed in federal court, the parties' Agreement, in Article 31.c.4, gives the Union the right to file a grievance on behalf of any employee or group of employees. Moreover, the Authority specifically rejected the Agency's argument in *AFGE, Local 1045 and United States Department of Veterans Affairs Medical Center, Biloxi, Mississippi,* 64 FLRA 86 (2010), stating as follows:

> Although the Agency cites *Parks v. IRS*, 618 F.2d 677, that decision is inapposite because it did not involve grievability under the Statute; it resolved the issue of whether the labor organization met the requisites for associational standing before a federal court.

Timeliness

The Agency also maintains that the Grievance is not timely. The Agency relies on Article 31, Section d of the Master Agreement, which states that, "Grievances must be filed within forty (40) calendar days of the date of the alleged grievable occurrence." [Joint Exhibit No. 1, p. 63.] The Agency reasons that, because the Grievance acknowledges notification on October 11, 2012 of the security problem and the Union did not file the Grievance until more than 40 calendar days after notification (November 29, 2012), the Grievance is untimely. However, as the Union contends, the Agency's position ignores relevant language in Article 31 of the Master Agreement.

Article 31, Section d of the Master Agreement states that, "A grievance can be filed for violations within the life of this contract, however, where the statutes provide for a longer filing period, the statutory period would control." [Joint Exhibit No. 1, p. 63.] [3] The Grievance alleges a violation of the Privacy Act, which states in relevant part as follows:

> An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises. . . . [5 U.S.C. § 552a (g)(5)]

There is no dispute that the Grievance was filed within two years of the cause of action, whether the cause of action is October 11, 2012, as the Agency contends, or

[3] The cases cited by the Agency on the timeliness issue are not on-point. The language of Article 31 with respect to statutes was not relevant to a decision in FMCS Case No. 06-54258 decided by Arbitrator Charles B. Overstreet, in FMCS Case No. 06-50931 decided by Arbitrator Richard Fincher, in FMCS Case No. 08-57010 decided by Arbitrator Samuel J. Nicholas, Jr., in FMCS Case No. 08-56151 before Arbitrator Paula Ann Hughes, or in FMCS Case No. 11-5218581 decided by Arbitrator Glen M. Bendixsen.

October 22, 2012, as the Union contends. Therefore, the Grievance is timely and arbitrable on the merits.

Merits

There is no dispute that there was a security breach that allowed documents containing private, sensitive information in the hands of inmates. Although the Agency does not acknowledge the security breach as a "disclosure" of employees' private information, the record clearly demonstrates that inmates had access to view and handle documents containing employees' private information during the recycling process. It is undisputed that the documents were records within a system of records.

There is also no dispute that the Privacy Act requires a showing that the agency acted in a manner which was "intentional or willful." [5 U.S.C. 552a(g)(4).] The Agency maintains that the security breach did not occur as a result of "intentional or willful" action by management.

As the Union contends, the U. S. Court of Appeals, 6th District held that the entire course of an agency's conduct is examined to determine if its disclosure was "intentional or willful." [*Beaven v. United States Department of Justice*, 622 F.3d (2010).] The Union also relies on the interpretation in *Maydak*, that "intentional or willful" is "somewhat greater than gross negligence, or committed without grounds for believing them to be lawful, or in flagrant disregard of others' rights under the Act." [*Maydak v. United States*, 630 F.3d 166, 180 (D.C. Cir. 2010).]

There is no dispute that inmates viewed and handled sensitive documents as part of FCC Butner's recycling program. There is no dispute that such handling of sensitive documents by inmates is contrary to policy, as acknowledged in the October 18, 2012

memorandum from the Agency's Assistant Director in the Information, Policy and Public Affairs Division, which states in relevant part as follows:

> The information Security staff in the Office of Information Systems has received reports of incidents where inmates are being used to handle sensitive documents – either as part of office operations (e.g. filing staff travel, training, or wellness forms) or as part of the institution's local recycling program. These practices are inconsistent with Program Statement 1237.13, "*Information Security*" that prohibits inmates from accessing sensitive data. Any activities at your institution that provide opportunities to inmates to access to such data must be discontinued immediately. [Footnote omitted as not relevant.]
>
> Please remind all staff of the following:
>
> ● Documents containing sensitive information (names, dates of birth, SSNs, home addresses, medical information, etc.) must be shredded;
>
> ● Inmates may not handle process or view sensitive information (e.g. filing, boxing, shredding, etc.). [Union Exhibit No. 7.]

As the Union submits, failure to comply with the policy that would have protected private information from inmates meets the standard of "intentional or willful" under the Privacy Act as interpreted in *Beaven v. U.S. Department of Justice*, 622 F.3d 540 (6th Cir. 2010). The 6th Circuit Court of Appeals affirmed the district court's judgment that a disclosure occurred and that the agency acted in a manner that was intentional or willful when a disclosure of private information occurred as a result of action contrary to policy. The Court engaged in a de novo analysis of the meaning of "intentional or willful" and considered Congress's intent, as demonstrated in the legislative history, regarding the language in § 552a(g)(4) of the Privacy Act. The Court concluded as follows:

> Consistent with the language of the Act, other courts' interpretations, and the legislative history, we conclude that a court may consider the entire course of conduct that resulted in the disclosure in making its required finding under § 552a(g)(4). Such an interpretation will allow recovery under circumstances similar to those here, where an agency's actions, although inadvertent at the last step, were in flagrant disregard of the

> plaintiff's rights under the Privacy Act at other steps along the way and afterward, but would deny recovery where an agency's actions were conscientious of Privacy Act rights throughout and contravened the Act inadvertently only at the last step – as where an employee with full rights to access personal information took every precaution to safeguard that information, but had it stolen and disclosed through no fault of his or her own while working away from the office.

It is reasonable to believe that the Agency did not intend for a privacy breach to occur. However, permitting inmates access to private information in the shredding process, disregarding the Agency's own policy, is not conscientious of Privacy Act rights and clearly constitutes a failure to take every precaution to safeguard private information.

The Agency relies on *Dowd v. IRS*, 776 F.2d 1083 (2d Cir. 1985), in which the court stated, "mere administrative error" in negligently destroying files was not a predicate for liability. Among many distinguishing facts, the decision in *Dowd* involved the destruction of files, not the disclosure of files as in the instant case. In *Dowd* the court of appeals upheld the district court's decision, finding that the appellants failed to demonstrate the IRS had any purpose for destroying the files and stating its unwillingness to predicate liability on a "mere administrative error." In the instant case, the disclosure of private information was not a "mere administrative error" but was the direct result of a failure to comply with policy that would have prevented the access by inmates to employees' private information during the shredding process.

The Agency maintains that the Grievance arose over the failure of a bargaining unit employee, the Recycling and Safety Technician, to safeguard sensitive information and that the grievance procedure is not intended to hold management liable for the shortcomings of a bargaining unit employee. The Agency maintains, "In fact, the undisputed evidence is that a former Recycling and Safety Technician, who was a

bargaining unit employee, was responsible for the archive boxes of documents to be shredded." [Agency's Post-Hearing Brief, p. 8.]

Agency witness Justin Andrews, who responded to the Grievance, testified that at the time of the breach, there was a staff member, who was a bargaining unit member, working at the recycling center. [Transcript p. 115.] Warden Andrews identified the staff member as Allison Harris and testified that she was terminated for having an inappropriate relationship with an inmate. [Transcript pp. 115-116.] As the Union contends, such testimony does not establish the Agency's claim that Harris was solely responsible for the security breach.

As the Union maintains, the evidence does not show that a single employee was solely responsible for the disclosure. Rather, the record demonstrates that the disclosure occurred as a result of inmates having access to employees' private information as part of FCC Butner's use of inmates in the recycling process. Moreover, as the Union also contends, even if one bargaining unit employee were found to be responsible for the disclosure, the Agency could be liable for a Privacy Act violation.

As the Agency contends, there are many ways for criminals to access personal information including home addresses. However, contrary to the Agency's argument, there is evidence to link the employees' financial issues to a security breach at the institution. As the Union contends, the necessity of taking time, outside of work, to register for credit monitoring, to contact banks and creditors, and to closely monitor credit occurred as a result of the security breach and the instruction by management following the security breach.

Contrary to the Agency's position, the Union's case is not based on pure speculation. As a result of the security breach and at the recommendation of the Agency, employees, on their own time, took action to protect their credit. The undisputed evidence demonstrates that employees were affected adversely, as required by the Privacy Act, 5 U.S. C. § 552 a(g)(1)(D). The record is undisputed that employees suffered actual lost time damages when they used their personal time to take preventative measures to protect their credit.

There is no dispute that, to recover under the Privacy Act, actual damages must be shown, i.e. pecuniary or material harm resulted from the security breach. As the Union contends, citing *Beaven*, 622 F.3d at 557-559, included in actual damages are the costs of prophylactic measures taken by a plaintiff to prevent harm from the disclosure as well as compensation for time spent dealing with the disclosure, calculated at the employee's regular hourly rate. There is no dispute that the Agency paid the cost of the credit monitoring. However, the time spent to register for the credit monitoring and other protective measures was on the employees' own time. As the Union contends, pursuant to 5 U.S. C. § 552a(g)(4), employees harmed by the violation are entitled to "(A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000 and (B) the costs of the action together with reasonable attorney fees as determined by the court."

Remedy

To avoid interference with the ongoing criminal investigation by the U. S. Attorney's Office, the hearing was bifurcated with regard to damages. The Union reserved its right

to receive all of the documents related to the criminal investigation before proceeding with the damages portion of the case.

Accordingly, and for the reasons stated, the Arbitrator finds for the Union and makes the following Award.

AWARD

The Arbitrator has jurisdiction to decide the Grievance. The Grievance is timely. The Agency violated the Privacy Act in October of 2012 by disclosing employees' personal information to inmates. The employees, whose information was disclosed, are entitled to actual damages or $1,000, whichever is greater. The Arbitrator retains jurisdiction to decide the damages if the parties are unable to do so following the completion of the criminal investigation and the release of relevant documents to the Union. The Arbitrator also retains jurisdiction to consider evidence and argument related to the Union's request for attorneys' fees, if the parties are unable to resolve the matter.

_____ DATE: April 10, 2015

Arbitrator