W&S

Wright, Constable & Skeen, L.L.P. | Attorneys at Law

Weekly Wright Report (1/22/18)

MARYLAND PERSONAL INFORMATION PROTECTION ACT

By Mike Stover

If your business collects "personal information" from your customers then you need to be aware of the Maryland Personal Information Protection Act, ("MPIPA") and the amendments that went into effect on January 1, 2018. The MPIPA applies to any "sole proprietorship, partnership, corporation, association, or any other business entity, whether or not organized to operate at a profit," including financial institutions and the parent or subsidiary of such financial institutions.

Under the MPIPA a covered business must protect personal information from unauthorized access, use, modification, or disclosure, by implementing and maintaining reasonable security procedures and practices that are appropriate to the nature of the personal information and the nature and size of the business and its operations. This obligation to protect personal information extends to nonaffiliated third-party service providers that perform services for the business as well.

Under the amendments to the Act, the definition of "personal information" now includes information such as names, social security numbers, driver's license numbers, bank account numbers, credit/debit card numbers, usernames/passwords, e-mail addresses, passport numbers, health insurance policy numbers, bio-metric data like fingerprints, voice print, genetic prints, retina scans, health information - including everything covered under HIPAA. Personal information does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records, information that an individual has consented to have publicly disseminated or listed, or information that is disseminated or listed in accordance with the HIPAA. Further, the personal information must be that of a customer which the Act defines as "an individual residing in the State who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business."

If there is a "breach of the security of a system," which is defined as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a business," the Act, requires the business, upon notification or discovery of the breach, to conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach. The Act as amended, also requires the business to notify the party owning the data no later than forty-five (45) days after the conclusion of the investigation that a breach has created a likelihood that the personal information has been or will be misused. The Act spells out in specific detail who is to be notified, the

7 Saint Paul Street, 18th Floor · Baltimore, Maryland 21202 · Phone: 410-659-1300 · Fax: 410-659-1350

method and manner of the notification and the nature of the notification.

In addition to protection of data and notification, the MPIPA also governs the destruction of records containing personal information of customers and employees and requires that when a business destroys such records it must take reasonable steps to protect against unauthorized access or use of the personal information by others.

A violation of the MPIPA is deemed an unfair or deceptive trade practice within the meaning of the Consumer Protection Act and a violator is subject to the enforcement and penalty provisions contained in Consumer Protection Act, including civil fines, penalties, criminal fines and penalties as well as attorney's fees.

MINIMIZING THE FINANCIAL IMPACT OF THE SHUT DOWN

By Don Walsh

Contractors should carefully document the effect of the shutdown on each of their contracts to calculate any necessary adjustments. Since the Government's authority to stop work is unilateral and can have severe consequences for a contractor, the equitable adjustment provisions and cost elements are often liberally applied. Although Contractors must always demonstrate an entitlement to the costs, accounting process and rules may not always be applied for Stop Work Orders since the decisions as to how to handle them are unique to management and generally considered outside the ordinary course of performance.

Contractors should perform a simple review of their records to identify the areas of their organization which were financially impacted. Items typically reviewed in these situations are:

- Idle time for employees working the project;
- Management costs which can be segregated to implement an orderly business approach to the stop work order internally and in coordination with the Government;
- Any severance pay triggered by the layoffs and/or increases in unemployment taxation rates by virtue of the complying with the order;
- Idle facility costs;
- Remobilization costs once the Stop Work Order is lifted;
- Any overtime which is necessitated by the remobilization;
- A calculation of any unabsorbed overhead which was not borne by other contracts during the stop work period; and
- Any costs of preparing, submitting, and negotiating the equitable adjustment, including costs of outside accountants, consultants and/or counsel.

As is the case with all equitable adjustments, the contractor is responsible for substantiating the reasonableness of the amounts requested.

EMPLOYERS BEWARE OF THE FCA ANTI-RELATIATION PROTECTIONS

By Mike Stover

The False Claims Act ("FCA") provides for private individual whistleblowers to file suit against parties engaging in fraud against the government. Indeed, suits by whistleblowers constitute the vast majority of claims filed under the FCA. To protect whistleblowers the Act

7 Saint Paul Street, 18th Floor · Baltimore, Maryland 21202 · Phone: 410-659-1300 · Fax: 410-659-1350

provides that retaliation against a whistleblower is prohibited. 31 U.S.C.A. § 3730(h). Specifically, the FCA provides that a whistleblower is entitled to "all relief necessary to be made whole," if that whistleblower is "discharged, demoted, suspended, threatened, harassed, or in any other manner discriminated against in the terms and conditions of employment" because of lawful acts done under the FCA. The relief that the whistleblower may be entitled to includes: (1) reinstatement with same seniority status; (2) double the amount of back pay lost; (3) interest on the back pay; and (4) compensation for any special damages sustained as a result of the discrimination, including litigation costs and reasonable attorneys' fees.

On December 22, the United States Court of Appeals for the Fourth Circuit in *O'Hara v. NIKA Technologies, Inc.*, 2017 WL 6542675 (4th Cir. Dec. 22, 2017) discussed the application of the anti-retaliation provision of the FCA in a unique circumstance. In *O'Hara* the whistleblower was not asserting an FCA complaint against his employer, rather the claim was against a subcontractor of his employer. The Fourth Circuit held that the FCA whistleblower protection provision does not condition protection on the employment relationship between a whistleblower and the subject of his disclosures. The Court stated that the language of the FCA indicates that protection under the statute depends on the type of conduct that the whistleblower discloses *i.e.*, a violation of the FCA, rather than the whistleblower's relationship to the subject of his disclosures. Thus, the Court concluded that the whistleblower is protected under the FCA even when their complaint is not against their employer. Ultimately, in *O'Hara* the Court ruled that the anti-retaliation provision did not apply because the whistleblower failed to prove that he was engaged in a "protected activity." To fall under the protection of the FCA, the whistleblower must demonstrate that the conduct disclosed reasonably could have led to a viable FCA action.

When dealing with a whistleblower under the FCA, employers must be cognizant of the anti-retaliation protections of § 3730(h) even if the whistleblower's claims are not directed at the employer.

7 Saint Paul Street, 18th Floor · Baltimore, Maryland 21202 · Phone: 410-659-1300 · Fax: 410-659-1350