RUTAN
RUTAN & TUCKER, LLP

Rutan & Tucker, LLP
611 Anton Blvd., Suite 1400
PO Box 1950
Costa Mesa, CA 92628-1950
(714) 641-5100 Fax (714) 546-9035
www.rutan.com

ORANGE COUNTY
PALO ALTO
(650) 320-1500
SAN FRANCISCO
(650) 263-7900
A PARTNERSHIP INCLUDING PROFESSIONAL CORPORATIONS

MEMORANDUM

CONFIDENTIAL: ATTORNEY-CLIENT PRIVILEGED COMMUNICATION AND ATTORNEY WORK PRODUCT

TO: Greg Morrell
President
Active Cypher
866-606-9814
3188 Airway, Suite D
Costa Mesa, CA 92627
gmorrell@activecypher.com

FROM: Michael Hellbusch

DATE: February 25, 2020

FILE NO.: 034183, 0001

RE: Active Cypher's Role In Ensuring "Reasonable" Security Procedures and Practices Pursuant to the California Consumer Privacy Act

---

Mr. Morrell,

This memorandum analyzes the role Active Cypher's data security solution, Active Cypher File Fortress ("ACFF"), plays in ensuring a robust information security program that is compliant with the California Consumer Privacy Act ("CCPA"), California Civil Code § 1798.100 *et. seq.*

1. Executive Summary

The Active Cypher File Fortress solution provides a comprehensive data security approach that combines various critical security controls into a single product. When implemented as part of a robust information security program, the ACFF can form a core part of a business's reasonable security procedures and practices necessary to achieve compliance under the California Consumer Privacy Act. By combining aspects of end-to-end encryption, with zero-trust identity centric attributes, Active Cypher enables businesses to seamlessly incorporate advanced data protection technologies with ease.

In implementing the CCPA, the California Legislature intended to make the determination of what constitutes reasonable security a fact-specific analysis to be decided on a case-by-case basis. In other words, whether a business's security procedures and practices are

reasonable depends on a multitude of factors. Nevertheless, the CCPA stresses the need for strong encryption schemes as part of an overall cybersecurity program. Active Cypher, which provides its proprietary Quantum Encryption Standard (QES) and the industry leading Advanced Encryption Standard (AES) encryption schemes for personal information integrated into operating parameters are derived from Active Directory information, is a formidable tool in demonstrating compliance with the CCPA and preventing data breaches from occurring. If properly implemented as part of an otherwise reasonable information security program, the Active Cypher technology can help demonstrate that a business has undertaken reasonable security procedures designed to comply with the CCPA.

In this memo, I first provide a high-level overview the CCPA. Next, I discuss the requirements to state a claim under the CCPA's private right of action and the business's duty to implement reasonable security procedures and practices. Finally, I discuss how the Active Cypher solution provides an effective means to employ encryption schemes to files containing personal information, and how that solution fits assists businesses in meeting their duty to implement reasonable security.

The CCPA is a new piece of legislation that is not yet being enforced. The California Attorney General has not issued any advisory opinions on the law and there is no case law interpreting the statute. Therefore, the interpretations I provide in this memo are not gospel, but are subject to change. Moreover, since the determination of whether the Active Cypher solution will be sufficient to demonstrate that the duty to use reasonable security procedures and practices depends on how the technology is used in practice, among other factors, I am not able to state that using the Active Cypher technology is, by itself, compliant with the CCPA. That said, I do believe that this cutting-edge technology is a valuable tool in effectuating reasonable security for most businesses.

2. The California Consumer Privacy Act

A. Summary of the CCPA

The CCPA is intended to require transparency from businesses about how and why they process personal information about individuals. The law provides California residents, (called "consumers" under the law) specific rights and imposes corresponding obligations on businesses who collect the personal information from those residents. The rights are as follows:

(1) The right to know what personal information is collected about them;

(2) The right to know if their personal information is shared or sold and to whom;

(3) The right to prohibit the sale of their personal information;

(4) The right to access their personal information;

(5) The right to have their personal information deleted; and

(6) The right to not be discriminated against for exercising their rights under the CCPA.

In addition to the aforementioned rights, the CCPA provides a private right to bring a civil action to any consumer whose "nonencrypted and nonredacted personal information" is subject to "an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." Cal. Civ. Code § 1798.150(a)(1). The next section will discuss this duty.

B. The CCPA's Duty to Implement Reasonable Security Procedures and Practices.

(1) The CCPA's Reasonableness Standard Should Be Interpreted Consistent With California's Existing Data Security Law, Which Is Based On Tort Law.

The California Legislature drafted the CCPA's reasonable security procedures and practices standard based on the well-established reasonableness standard in tort law. This is evident in several ways, but primarily by the fact that the CCPA expressly borrows from the state's existing data security statute, the California Consumer Records Act ("CRA"), Cal. Civ. Code 1798.81.5, which employs a reasonableness standard based on common law tort claims.[1] In addition, the CCPA states that the law is meant to

[1] *See* Cal. Civ. Code § 5 "The provisions of this Code, so far as they are substantially the same as existing statutes or the common law, must be construed as continuations thereof, and not as

"further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information, including...Title 1.81 [which includes the CRA].

The CRA requires certain businesses to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information [.]" Cal. Civ. Code 1798.81.5. The CRA's legislative history explains that the "reasonableness" standard described in the statute is based on reasonableness standard well-established in tort law. *See Privacy: Personal Information, Hearing on A.B. 1950 Before the S. Comm. on the Judiciary,* 2003-2004 Leg., Reg. Sess. 4 (Cal. 2004) ("[T]he goal of the bill is to provide a minimum standard of protection to personal information not covered by existing privacy laws. The bill would not set forth a specific standard, but instead rely on the 'reasonableness' standard already well-established by tort law.").

Some have argued the CCPA's reasonable security standard is intended to codify a rigid cybersecurity framework, namely the Center for Internet Security's Critical Security Controls ("CIS Controls"). While such reasoning is understandable, the Attorney General's Office has previously endorsed the CIS Controls as the "minimum level of information security" that organizations should meet, it is erroneous.[2] The California Data Breach Report is self-described as "informational" document only. However, that does not mean the Report is unhelpful. To the contrary, as demonstrated herein, the CIS Controls are helpful in establishing what industry standards are, and can serve as instructional guidance as to what plaintiffs' attorneys will argue contemplates the minimum standards of data protection.

Therefore, when reading the CCPA as a whole, it is clear the intent of the legislature was to utilize the existing understanding of a flexible reasonableness standard in the CRA, which is based on tort law.

---

new enactments."

[2] In the California Department of Justice, Attorney General's Office, California Data Breach Report (Feb. 2016), then Attorney General Kamala Harris wrote: "The 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security."

Greg Morrell
President
Active Cypher
866-606-9814
3188 Airway, Suite D
Costa Mesa, CA 92627
gmorrell@activecypher.com

(2) The "Reasonableness Standard" Is That Of The Ordinary [Non-Expert] Reasonable Person.

The duty to use reasonable care, when implementing security procedures or otherwise, is based on the common law understanding of the "ordinary prudent or reasonable person." *Summary of California Law* (WITKIN, 11th ed. 2019) section 998. When applying this concept to the CCPA's reasonable security procedures and practices standard, the questions becomes how a business balances the risk of foreseeable injury to a consumer and the business's ability to control such risk. When adding the requirement that the business evaluate security "appropriate to the nature of the information," the Legislature sought to codify the concept that there is a heightened risk of harm to the consumer if certain personal information is breached. As a result of this heightened risk, the duty of care owed to individuals obliges businesses implement security procedures specific to the mitigate those risks. Nevertheless, the security measures must still be reasonable under the circumstances.

Case discussing the pleading requirements under the CRA have not so much defined what reasonable security is, but instead have defined what it is not. For example, allegations that the business failed to implement any encryption scheme have been sufficient to plead a breach of the duty to implement reasonable security. *See In re Sony Gaming Networks*, 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014) ("As a result, because Plaintiffs allege that they provided their Personal Information to Sony as part of a commercial transaction, and that Sony failed to employ reasonable security measures to protect their Personal Information, including the utilization of industry-standard encryption, the Court finds Plaintiffs have sufficiently alleged a legal duty and a corresponding breach."). Other cases have held that allegations that the business failed to *properly implement* encryption schemes is sufficient to plead a breach of the duty. In I*n re Adobe Systems Privacy Litigation*, the Northern District of California found standing to assert a CRA claim based on allegations that Adobe's encryption scheme was "poorly implemented." *In re Adobe Sys., Inc.*, 66 F. Supp. 3d 1197, 1206-07 (N.D. Cal. 2014). That allegation, combined with other allegations that Adobe failed to implement other common, industry-standard security controls that resulted in the breach of plaintiffs' information, was sufficient to state a claim.

In order to state a claim under the CCPA, plaintiffs likely must demonstrate the security measures put in place are unreasonable. Based on the analysis above,

unreasonableness is properly alleged if a business fails to properly implement, or implement at all, an encryption scheme. Ultimately, the determination of whether a business's security procedures and practices is reasonable under the circumstances is a question of fact. However, businesses that want to quickly dispose of claims under the CCPA or CRA breach standards should ensure, at a minimum, that *some* level of encryption is applied to personal information. The failure to implement any encryption scheme will be fatal precluding claims under the CCPA.

C. Encryption Schemes As Part of Reasonable Security Procedures and Practices.

The CCPA ostensibly provides a safe harbor from statutory liability if the consumers' personal information subject to a data breach is encrypted *and* redacted. Civ. Code § 1798.150(a)(1). There is some ambiguity as to whether the Legislature intended to require encryption *and* redaction rather than encryption *or* redaction. For instance, the definition of personal information that is to be used in Section 1798.150 is that established in the CRA, which defines personal information to include certain data elements that are "not encrypted or redacted." Civ. Code § 1798.81.5(d)(1)(A). The CCPA does not define or elaborate on the term "encryption," but we should understand the term to mean the process of obscuring information in order to make the information unreadable without special knowledge. In other words, encryption is the process of changing plaintext into cyphertext for the purpose of security or privacy. *See NIST SP-800-175.B.*Nevertheless, the statute facially requires both. For purposes of this memorandum, I will focus solely on the encryption requirement.

The CCPA's encryption and redaction safe harbor should be read in conjunction with its reasonable security requirements. The fact that particular data elements are encrypted and redacted will likely not provide safe harbor if, as a result of the failure to implement and maintain reasonable security practice and procedures, the encryption keys have also been compromised. The key management system for the particular encryption scheme must be evaluated in light of what is reasonable. California's breach notification law, Cal. Civ. Code §1798.82, includes a notification requirement when the encryption key or security credential used to unencrypt the data is also obtained by an unauthorized party. Therefore, business must also consider key management as part of their overall security posture. Simply having encryption is insufficient under the CCPA if the business

fails to ensure that the encryption scheme prevents data from being subject to unauthorized access and use, theft, or disclosure.

Not all encryption schemes are equal. In fact, certain encryption schemes have been deemed outdated or insecure given the advances in code-breaking technology. For example, the Data Encryption Standard (DES), which became effective in 1977, and was the first NIST -approved cryptographic algorithm, is no longer considered sufficient to adequately protect Federal Government data, due to advances in computer power and speeds. DES was withdrawn as an approved algorithm in 2005. *See NIST.SP.800-175B.* Logically, encryption schemes which prove most resilient to code-breaking technologies will be considered secure.

Currently, the Advanced Encryption Standard (AES) is widely considered to be a highly secure (and FIPS-approved) cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt and decrypt information. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. An encryption standard which surpasses AES' cipher capabilities would be deemed highly advanced and thus beyond the industry-standard levels of encryption. Neverthless, whether a particular encryption algorithm is "reasonable" for a particular application will be a question of fact, but the ultimate question is whether the encryption scheme maintained the obscurity of the information. If such is the case, then the personal information cannot be deemed "nonencrypted."

3. **Active Cypher's Solutions Are Effective Tools in Demonstrating Reasonable Security as defined by the CCPA.**

As described, above, the CCPA's reasonable security standard requires, at a minimum, a level of encryption that preserves the confidentiality of the personal information encrypted. As stated in the documentation, Active Cypher's Quantum Encryption Standard (QES), a proprietary security algorithm, utilizing a virtual one-time pad, provides greater security, randomness and obfuscation than AES. If true, such a standard would exceed the industry-standard AES in terms of encryption capability. Since a consumer's ability to bring a cause of action under the CCPA is predicated upon his breached information being "nonencrypted," a product, like Active Cypher, that can offer enhanced levels of encryption technology is extremely valuable.

In addition, Active Cypher leverages deep integration with Microsoft's Azure and Active Directory to combine key critical security controls into a single solution. The Active Cypher solution places all key access and management governance within the customer's Azure Tenant. No third party has access to keys. Active Cypher only tracks the *number* of keys licensed to the client. Finally, Active Cypher decryption requires several verification and validation processes be performed prior to usage of the keys. This solution, as part of an overall cybersecurity arsenal, can provide strong evidence that a business has implemented and maintain reasonable security procedures and practices in accordance with the CCPA.

4. Conclusion

Active Cypher's cutting-edge technology solutions are powerful tools in preventing a "breach" under the CCPA. The cutting edge technology addresses the core challenge in ensuring that a business is not liable under the CCPA for a data breach: Ensuring that personal information is securely encrypted. But Active Cypher does more than simply encrypt data in a highly secure fashion, it leverages industry-established tools like Azure and Active Directory to ensure that access controls are properly governed. As part of a robust information security program, Active Cypher is an optimal tool for demonstrating compliance with the CCPA's reasonable security requirements.