nCIPHER
AN ENTRUST DATACARD COMPANY

www.ncipher.com

nCipher helps enterprises comply with key requirements of California's Consumer Privacy Act (CCPA) and Data Breach Notification Statute by managing and securing encryption keys

Complying with California's Consumer Privacy Act and Breach Notification Statute

SUMMARY

The California Consumer Privacy Act (CCPA)[1] went into effect at the beginning of 2020, and July 1, 2020 marks the expiration of the six-month CCPA compliance grace period. The CCPA addresses the use of encryption to protect consumer personal information. In its definitions, the CCPA also references Assembly Bill 1130[2], which updates the California breach notification statute and which requires sending formal notifications to people whose data has been breached unless that data was encrypted and the encryption keys were not obtained with the data.

Those found in violation of CCPA stand to incur a $7,500 fine for each intentional violation. Non-intentional violations are less onerous, but still costly, at $2,500 each. However, civil litigation can potentially have a very negative impact on non-compliant organizations. For each consumer affected by CCPA non-compliance, organizations stand to face up to $750 in civil damages *per consumer*.

Complying with California's Consumer Privacy Act and Breach Notification Statute

CONSUMER DATA PROTECTION

Section 1798.150. (a) (1) of the CCPA states:

> Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, 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 may institute a civil action for any of the following:
>
> (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.
>
> (B) Injunctive or declaratory relief.
>
> (C) Any other relief the court deems proper.

While the CCPA itself does not provide more details about data encryption, an amendment to California's **data breach statute**, does. Late in 2019, simultaneous to signing amendments to CCPA, California's legislators also signed Assembly Bill 1130, which specifically refers to encryption and the protection of encryption keys. The following is excerpted from the Bill:

> **Section 1789.82 of the Civil Code is amended to read:**
>
> **1798.82.** (a) A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California **(1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable.** The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

HOW NCIPHER CAN HELP YOU COMPLY WITH CCPA AND AVOID THE DATA BREACH NOTIFICATION REQUIREMENT

Key protection

The amendment above indicates organizations cannot just encrypt California residents' data to protect it, they must also safeguard the associated encryption keys or security credentials to be in compliance. Encryption protects sensitive information, including financial data, government IDs and Social Security numbers, by making it unreadable, but if you fail to protect the encryption keys it's like locking your front door and leaving the keys under the mat.

nCipher solutions for cryptographic key security

Best practice for cryptographic key security is to store those keys in a hardware security module (HSM). nCipher's nShield HSMs are hardened, tamper-resistant hardware devices that secure cryptographic processes by generating, protecting, and managing keys used for encrypting and decrypting data and creating digital signatures and certificates. These HSMs are tested, validated and certified to the highest security standards including FIPS 140-2[3] and Common Criteria[4]. nShield HSMs enable organizations to:

- Meet and exceed established and emerging regulatory standards for cybersecurity, including CCPA[5], GDPR[6], eIDAS[7], PCI DSS[8], HIPAA[9], etc.
- Achieve higher levels of data security and trust
- Maintain high service levels and business agility

nShield as a Service is a subscription-based solution for generating, accessing and protecting cryptographic key material, separately from sensitive data, using dedicated FIPS 140-2 Level 3 certified nShield Connect HSMs. The solution delivers the same features and functionality as on-premise HSMs combined with the benefits of a cloud service deployment. This allows customers to fulfill their cloud first objectives and leave the maintenance of these appliances to the experts at nCipher.

FOR MORE INFORMATION

For more detailed information on these products, please visit www.ncipher.com

ABOUT NCIPHER SECURITY

nCipher Security, an Entrust Datacard company, is a leader in the general-purpose hardware security module (HSM) market, empowering world-leading organizations by delivering trust, integrity, and control to their business-critical information and applications. Today's fast-moving digital environment enhances customer satisfaction, gives competitive advantage, and improves operational efficiency, but it also multiplies security risks. Our cryptographic solutions secure emerging technologies, such as cloud, IoT, blockchain, and digital payments and help meet new compliance mandates. We do this using the same proven nCipher technology that global organizations depend on today to protect against threats to their sensitive data, network communications, and enterprise infrastructure. We deliver trust for your business-critical applications, ensure the integrity of your data, and put you in complete control – today, tomorrow, always. www.ncipher.com

1. http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=
2. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1130
3. https://www.ncipher.com/solutions/compliance/americas/fips-140-2
4. https://www.ncipher.com/products/product-certifications/common-criteria
5. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1130
6. https://www.ncipher.com/solutions/compliance/global/gdpr
7. https://www.ncipher.com/solutions/compliance/emea/eidas
8. https://www.ncipher.com/solutions/compliance/global/pci-dss
9. https://www.ncipher.com/solutions/compliance/americas/hipaa

Search: nCipherSecurity

nCipher AN ENTRUST DATACARD COMPANY