[DATE]

[INDIVIDUAL NAME]
[STREET ADDRESS]
[CITY, STATE AND POSTAL CODE]

NOTICE OF DATA BREACH

Dear [INDIVIDUAL NAME]:

CVC Holding Corp recently experienced a cybersecurity event. Please read this notice carefully, as it provides up-to-date information on what happened and what we are doing in response.

WHAT HAPPENED?

On November 1, 2023, CVC became aware of a network-wide cybersecurity event (the "Incident"). Upon detection, CVC took immediate steps to block any unauthorized access to its network and an investigation of the Incident was launched with the support of leading outside cybersecurity experts. The outside cybersecurity experts determined that CVC had been a victim of a "LockBit 3.0" ransomware group ("LockBit Group") attack. Ransomware is a type of computer virus that prevents users from accessing their network either by locking the user's computer screen or by locking the user's computer files.

Based on our investigation we have determined that as a result of the attack, the LockBit Group ***may have*** obtained access to CVC files containing your personal information on November 1, 2023. Based on the available evidence, the outside security experts determined that any LockBit Group access to the CVC network was likely limited to November 1, 2023. Note that on November 6, 2023, the LockBit Group briefly posted a notice on the internet regarding its attack on CVC, albeit without any disclosing any CVC data.

WHAT INFORMATION WAS INVOLVED?

The personal information the LockBit Group ***may have*** accessed ***could*** include: (1) your social security number (2) your driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify your identity (3) your medical information, including a medical identification number; and (4) your health insurance information, including a health insurance identification number. Please note that not all personal information may have been involved for all individuals. In addition, to date, CVC is not aware of any actual fraud or identity theft instances involving your personal information.

WHAT WE ARE DOING

CVC is conducting a thorough review of the potentially affected systems and has implemented additional security measures designed to prevent a recurrence of such an attack. The outside cybersecurity experts have also confirmed to CVC with a high level of confidence the successful removal of the LockBit Group from CVC's network.

Additionally, CVC is offering you one year of complimentary credit monitoring and identity restoration services through Experian. To take advantage of these free credit monitoring and identity theft protection services, please follow the instructions provided on Attachment A to this letter. You must enroll by 5:59 p.m. CT on March 1, 2024 to receive these complimentary services.

WHAT YOU CAN DO

Please also review Attachment A to this letter for further information on steps you can take to protect your information, and how to receive free credit monitoring/identity theft protection services for one year from Experian.

FOR MORE INFORMATION

For further information and assistance, you may contact us at 916-852-6030 between 8 a.m.- 4 p.m. PST on business days, by emailing contact@concretevalue.com, or by contacting us at the address below.

Sincerely,

Nathan Esch, CEO
CVC Holding Corp
530 Bercut Drive, Ste G
Sacramento, Ca. 95811

Attachment A

Steps You Can Take to Further Protect Your Information

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. We recommend that you promptly change your password, security question or answer for any accounts affected by the data incident. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **Obtain and Monitor Your Credit Report**

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(866) 349-5191	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241 Atlanta, GA 30374	P.O. Box 2002 Allen, TX 75013	2 Baldwin Place P.O. Box 1000 Chester, PA 19016

- **Consider Placing a Fraud Alert on Your Credit Report**

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

- **Credit Report Monitoring/Identity Theft Protection Services from Experian**

What we are doing to protect your information:
To help protect your identity, we are offering a complimentary 12-month membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: 5:59 p.m. CT on March 1, 2024 (your code will not work after this time)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: **[ACCESS CODE]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian. A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance[2]:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 12-months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

- **Take Advantage of Additional Free Resources on Identity Theft**

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://consumer.ftc.gov/identity-theft-and-online-security.

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338).

OTHER IMPORTANT INFORMATION

- **Security Freeze**

You have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. There is no charge to request a security freeze or to remove a security freeze.

[1] Offline members will be eligible to call for additional reports quarterly after enrolling

[2] The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.