<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

December XX, 2025

Cybersecurity Incident

Dear <<Full Name>>,

K-Log values your business and respects the privacy of information relating to your business and employees, which is why, as a precautionary measure, we are writing to inform you of a cybersecurity incident that may involve information relating to your business or employees. We are providing information about the incident, measures K-Log has taken in response to the incident, steps you can take to help protect yourself against possible misuse of information, and steps K-Log will take to assist you.

We sincerely apologize for any inconvenience this incident may cause your business or employees.

**What Happened**

On or about October 28, 2025, K-Log's website was attacked via the internet by unknown actors. Malware was surreptitiously installed on our webserver that copied user inputs or retrieved stored data and transmitted the data to an unknown party/ies. After detecting the unauthorized code, we proactively took our systems offline to contain the threat. We removed the malware and installed new software to prevent this sort of unauthorized access in the future.

Unfortunately, our investigation identified signs that data was copied and may have been taken from K-Log's webserver between October 24 to November 7, 2025. We determined on November 10 that the data at issue may contain information relating to your business or employees.

**What Information Was Involved**

The information in the data at issue may include credit card numbers, expiry dates, and CVV codes manually entered during the checkout process. Additionally, previously stored data may have been exposed if the account was accessed during the affected period. This would include first/ last names, physical and email addresses, telephone numbers, tax-exempt status, business tax identification numbers and account passwords.

K-Log does not store credit card information online (or offline), and there are no indications that our enterprise software was affected by this breach. As far as we can determine, only data input online and/or previously stored data for accounts accessed during the period affected by this breach was compromised.

We are not aware of any misuse of information relating to your business or employees resulting from this incident.

**What We Are Doing**

K-Log took immediate steps to secure our webserver, remove malware, and remediate compromised files. Further, in response to this incident, we implemented additional cybersecurity safeguards to our existing robust infrastructure to minimize the likelihood of a recurrence.

**What You Can Do**

We recommend that you remain vigilant, monitor and review all financial and account statements, and report any unusual activity to the institution that issued the credit card and to law enforcement. You may also review the guidance contained in the attached *Steps You Can Take to Protect Personal Information.*

Additionally, as a courtesy, K-Log is providing you with the opportunity to register for two (2) years of credit monitoring and identity protection services at our expense. Please contact us so that we can assist you in setting up this service by phone at (800) 872-6611 or email privacy@k-log.com.

**For More Information**

The security of your personal information is a top priority for us. We sincerely regret this incident occurred and for any concern it may cause you. We understand that you may have additional questions. For assistance with questions regarding this incident, please call K-Log at (800) 872-6611 or email privacy@k-log.com. Representatives are available between the hours of 7:00 am to 6:00 pm Central time, Monday through Friday (excluding U.S. holidays).

Sincerely,

Linda Lester
Vice President

**STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION**

**Enroll in Monitoring Services**

Please contact us so that we can assist you in setting up this service by phone at (800) 872-6611 or email privacy@k-log.com.

**Monitor Your Accounts**

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

| **Equifax** | **Experian** | **TransUnion** |
|---|---|---|
| https://www.equifax.com/personal/credit-report-services/ | https://www.experian.com/help/ | https://www.transunion.com/credit-help |
| 1-888-298-0045 | 1-888-397-3742 | 1-800-916-8800 |

| | | |
|---|---|---|
| Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069 | Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013 | TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016 |
| Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788 | Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013 | TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094 |

**Additional Information**

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.