

<<INGO LOGO HERE>>

<<FirstName>> <<LastName>>

<<Date>> (Format: Month Day, Year)

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip Code>>

Re: Notice of Data Breach

Dear <<FirstName>> <<LastName>>:

Ingo Money provides check risk management and related services as a vendor to [[<<Service Provider Company Name >>](#) OR [<<General Description: various financial institutions>>](#)] in support of their check cashing services, which you used to cash a check. We are writing to inform you about a data security incident that involved some of your personal information associated with the Ingo Money services and those services we provide to your financial institution.

What happened? On or about November 23, 2023, we were notified that an unauthorized third-party publicly disclosed certain information. Outside cyber professionals promptly investigated – discovering that an unauthorized third-party removed data sometime in the weeks before from a limited portion of our corporate computer network.

What information was involved? An outside review was conducted to assess the data involved and to identify individuals requiring notification. On [<<NCOA date>>](#), we obtained your name and current mailing address to be able to notify you that posted files may include elements such as your name, [<<data elements>>](#). This information varies by individual.

What we are doing. As part of the investigation, outside technical experts were engaged and further enhanced the security of our systems. Law enforcement was notified. Our security team and third-party cyber professionals will continue to closely monitor our systems 24/7/365 for any unusual activity. **We are notifying you out of an abundance of caution, and for your peace of mind, we are offering you [<<12 months or 24 months>>](#) of free credit monitoring and \$1 million in identity theft insurance.**

What you can do. We encourage you to take advantage of the free credit monitoring services offered. In the “Additional Resources” section included with this letter, you will find additional steps you may wish to take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your accounts or credit file. We recommend you always remain vigilant and as a matter of good financial hygiene, we encourage you to regularly review your account statements and promptly report and dispute any discrepancies to the applicable financial institution. **Please note: You must activate the [<<Epiq>>](#) product by the activation date for it to be effective. The activation instructions are included with this notification.**

For more information, you may call toll free [<<1-???-???-????>>](#), Monday through Friday from [<<8:00 a.m. to 5:30 p.m. Central Time,>>](#) excluding major U.S. holidays. We are fully committed to protecting your personal information and sincerely apologize for any concern this incident may have caused you.

Sincerely,

Name and Title

Additional Resources

add EPIQ instructions – ID theft

ADDITIONAL STEPS YOU MAY WISH TO TAKE

- **REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS & REPORT FRAUD AND IDENTITY THEFT. CHANGE PASSWORDS AND SECURITY VERIFICATION QUESTIONS & ANSWERS.** It is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your credit reports, debit/credit card, insurance policy, bank account and other account statements for unauthorized activity— especially over the next 24 months. Activate alerts on your bank accounts to notify you of suspicious activity and change passwords/security verifications as needed – particularly if same password is used over multiple online accounts. If your medical information was involved, it is also advisable to review the billing statements you receive from your healthcare providers. Immediately report suspicious activity, fraudulent charges, or suspected identity theft in your insurance statements, provider billing statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor, healthcare provider and law enforcement, including FTC and/or your State Attorney General.
- **FREEZE YOUR CREDIT FILE.** You have a right to place a 'security freeze' on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, using a freeze to take control over who gets access to the personal/financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application made regarding a new loan, credit, mortgage, or any other account involving extension of credit. Security freeze generally does not apply to existing account relationships and when a copy of your report is requested by existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. It is free to place, lift, or remove a security freeze. To place a security freeze on your credit report, contact each of the following credit bureaus and clearly explain in the call/letter that you are requesting a security freeze:
 - *Equifax*, PO Box 105788, Atlanta, GA 30348, www.equifax.com, 1-800-685-1111
 - *Experian*, PO Box 9554, Allen, TX 75013, www.experian.com, 1-888-397-3742
 - *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

To request a security freeze, provide your full name (middle initial, Jr., Sr., II, III, etc.), Social Security Number, date of birth; home addresses over the past 5 years; proof of current address such as a current utility bill or telephone bill; photocopy of government issued identification card (driver's license or ID card, military ID, etc.); and if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. If you request a security freeze via toll-free telephone or other secure electronic means, credit reporting agencies have 1 business day after receiving the request to place the freeze. In the case of a request made by mail, the agencies have 3 business days after receiving your request to place a security freeze on your credit report. Credit agencies must also send written confirmation within 5 business days and provide a unique personal identification number (PIN) or password, or both that can be used to authorize the removal or lifting of the security freeze. To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and PIN or password provided when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receiving a request to lift freeze for those identified entities or for the specified period of time. To remove the freeze, you must send a written request to the 3 credit bureaus by mail and include proper identification (name, address, & social security number) and PIN number or password provided when you placed the freeze. The credit bureaus have 3 business days after receiving the request to remove the freeze.

- **PLACE FRAUD ALERTS ON YOUR CREDIT FILE.** As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is an alert lasting 7 years. Contact the 3 credit reporting agencies listed above to activate an alert.

- **ORDER FREE ANNUAL CREDIT REPORTS.** Visit www.annualcreditreport.com or call 877-322-8228 to obtain 1 free copy of your credit report annually. Periodically review a copy of your credit report for discrepancies and identify accounts you did not open or inquiries you did not authorize. For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) copies of your credit report, free of charge. You must contact each of the 3 credit reporting agencies directly to obtain such additional reports.
 - *Equifax*, PO Box 105281, Atlanta, GA 30348, www.equifax.com, 1-800-685-1111
 - *Experian*, PO Box 9554, Allen, TX 75013, www.experian.com, 1-888-397-3742
 - *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800
- **OBTAIN POLICE REPORT:** You have a right to a police report about this incident (if any exists). If you are an identity theft victim, you have the right to file a police report and obtain a copy of it. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Notification of this incident has not been delayed as a result of a law enforcement investigation.
- **SUMMARY OF YOUR RIGHTS UNDER FAIR CREDIT REPORTING ACT (FCRA):** FCRA promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552. (1) You must be told if information in your file has been used against you. (2) You have the right to know what is in your file. (3) You have the right to ask for a credit score. (4) You have the right to dispute incomplete or inaccurate information. (5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. (6) Consumer reporting agencies may not report outdated negative information. (7) Access to your file is limited. (8) You must give your consent for reports to be provided to employers. (9) You may limit “prescreened” offers of credit and insurance you get based on information in your credit report. (10) You have a right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. (11) You may seek damages from violators. (12) Identity theft victims and active-duty military personnel have additional rights.
- **FEDERAL TRADE COMMISSION AND STATE ATTORNEYS GENERAL OFFICES.** If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General’s office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft. You may contact the Federal Trade Commission at www.ftc.gov/idtheft; FTC hotline is 877-438-4338; TTY: 1-866-653-4261 or write to FTC, 600 Pennsylvania Ave., NW, Washington, D.C. 20580. Additional information for the residents of the following states:
 - **Connecticut:** You may contact and obtain information from your state attorney general at: Connecticut Attorney General’s Office, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag
 - **District of Columbia:** You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 400 6th Street, NW, Washington, DC 20001, 1-202-727-3400, databreach@dc.gov, www.oag.dc.gov
 - **Maryland:** You may contact and obtain information from your state attorney general at: Maryland Attorney General’s Office, 200 St. Paul Place, Baltimore, MD 21202, 1-410-576-6300; <https://www.marylandattorneygeneral.gov> Consumer Hotline 1-410-528-8662, or consumer@oag.state.md.us.
 - **Massachusetts:** You have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-2200, www.mass.gov/ago/contact-us.html
 - **New York:** You may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>
 - **North Carolina:** You may contact and obtain information from your state attorney general at: North Carolina Attorney General’s Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh,

Ingo Money – Consumer Notice Letter – Service Provider – Credit Monitoring

NC 27699, 1-919-716-6000/ 1-877-566-7226, www.ncdoj.gov

- **Rhode Island:** Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov. (Approximately <<INSERT NUMBER>> Rhode Island residents were impacted by this incident.)
- **West Virginia:** You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" on your file and let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

SAMPLE DRAFT