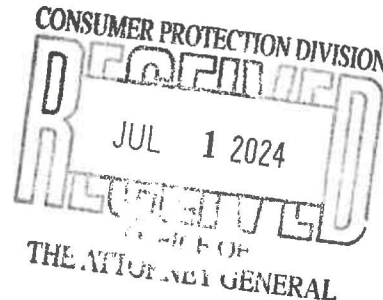


Gina G. Greenwood
T: 478.387.0458
gina.greenwood@nelsonmullins.com

201 17th Street NW, Suite 1700
Atlanta, GA 30363
T: 404.322.6000 F: 404.322.6050
nelsonmullins.com



June 25, 2024

Attorney General Anthony Brown
200 St. Paul Place
Baltimore, MD 21202

Re: Ingo Money, Inc. - Notice of Data Breach

Dear Attorney General Anthony Brown:

I serve as outside legal counsel to Ingo Money, Inc. (“Ingo Money”), which provides check risk management and related services to various financial institutions and check cashers, with its principal office located at 11545 Wills Rd., Ste. 130, Alpharetta, GA 30009.¹

This correspondence is to notify you of a recent security incident at Ingo Money, details of which are described in the example notice letter enclosed for your reference, which includes the following:

- A description of the security event;
- Steps taken to investigate;
- Steps taken to mitigate any potential harm to consumers;
- As applicable, instructions for activating free identity and credit monitoring services that include identify theft restoration, triple bureau credit monitoring, fraud consultation, and a \$1 million insurance reimbursement policy to all consumers who received notification;
- Instructions on how to place a security freeze on the recipient’s consumer credit report; and
- Instructions regarding how to obtain more information about this event, etc.

The incident affected a small subset of corporate servers housed in Ingo Money’s corporate environment.

This incident did not affect any payment activity or Ingo Money apps. Further, the incident did not affect Ingo Money payment or check processing systems. Of note, aside from Ingo Money, no other companies’ systems were impacted by this incident.

In an abundance of caution, notification will be sent to 389 residents of your State on or about June 26, 2024. The notification letters include instructions for activating credit monitoring services, where required by law, at no cost to the recipients. The personal information that was potentially at risk varied by individual and may have included elements such as first and last name, address, social security number, driver’s license, and other financial related information.

¹ By providing this notice, Ingo Money does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

June 25, 2024

Page 2

Ingo Money is fully committed to protecting the privacy and confidentiality of personal information. Ingo Money continues to work with outside technical experts to further enhance its systems' security, including 24/7/365 monitoring for any unusual activity.

We will follow up this correspondence with any forms or other documents that may need to be completed. Please contact me if you require any additional information regarding this incident.

Best regards,

Gina G. Greenwood

Gina G. Greenwood

Enclosure:

Example Notification Letter (Credit Monitoring Version)

June 25, 2024

Page 3

<<INSERT LOGO HERE>>

<<First Name>> <<Last Name>>

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

<<Street Address>>

<<Street Address Two>>

<<City>>, <<State>> <<ZIP/Postal Code>>

Recipient ID: <<Breach ID>>

Re: NOTICE OF DATA BREACH

Dear <<First Name>> <<Last Name>>:

Ingo Money, Inc. provides check risk management and related services as a vendor to various financial institutions in support of their check cashing services. You cashed a check using one of these financial institutions through a mobile app for a prepaid card or an electronic wallet.

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 others.

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 discovery from a limited portion of our corporate computer network. Aside from Ingo Money, no other financial institution or company's computer systems were impacted by this incident.

What information was involved? An outside review was conducted to assess the data involved and to identify individuals requiring notification. On June 21, 2024, 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 and the relationship of the parties vary 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.

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, if you feel necessary. 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 and law enforcement. **Please note: You must activate the credit monitoring product by the activation date for it to be effective. Activation instructions are included with this notification.**

For more information, you may call toll free <<insert dedicated telephone number>>, 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,

Rusty Pickering
President and Chief Operating Officer

ADDITIONAL RESOURCES

- **ACTIVATE FREE IDENTITY MONITORING SERVICES:** We have secured Kroll identity monitoring at no cost to you for <<one year/two years>>. Kroll is a global leader in risk mitigation and response, and its team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.
- Visit <<IDMonitoringURL>> to activate and take advantage of your identity monitoring services.
 - You have until <<Date>> to activate your identity monitoring services.
 - Membership Number: <<Member ID>>
 - For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Specifically, upon activation, you have access to the following services from Kroll:

- **Triple Bureau Credit Monitoring:** You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.
- **\$1 Million Identity Fraud Loss Reimbursement:** Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.
- **Fraud Consultation:** You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.
- **Identity Theft Restoration:** If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can help resolve issues.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the US, have a social security number in your name, and have a US residential address associated with your credit file.

- **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*, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com, 1-800-685-1111
- *Experian*, P.O. Box 9554, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, P.O. 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, or 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*, P.O. Box 105281, Atlanta, GA 30348, www.equifax.com, 1-800-685-1111
 - *Experian*, P.O. Box 9554, Allen, TX 75013, www.experian.com, 1-888-397-3742
 - *TransUnion*, P.O. 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 FEDERAL 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). You have rights under FCRA that 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 credit 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.

- **CONTACT LAW ENFORCEMENT, FEDERAL TRADE COMMISSION (FTC), AND STATE ATTORNEY GENERAL.** 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 law enforcement, the FTC and/or the Attorney General’s office in your home state. You may also contact these agencies for information on fraud alerts and security freezes and how to prevent or minimize the risks of identity theft. You may contact the FTC 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. Below is additional information for residents of the following states:

- **Connecticut:** You may contact and obtain information from 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 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
- **Iowa:** You are advised to report any suspected identity theft to law enforcement or Iowa Attorney General, 1305 E. Walnut Street, Des Moines, IA 50319, <https://www.iowaattorneygeneral.gov>, 515-281-5926 or 888-777-4590.
- **Maryland:** You may contact and obtain information from your state attorney general at Maryland Attorney General’s Office – Consumer Protection Division, 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. You may contact Ingo Money directly at 11545 Wills Rd, Ste 130, Alpharetta, GA 30009 <<Insert Ingo Money Direct Phone Line>>
- **Massachusetts:** You may contact and obtain information from Office of Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html. The mitigation services outlined above are offered pursuant to Mass. Gen. Laws Ann. Ch.93H, § 3(b).
- **New York:** You may contact and obtain information from 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 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 North Carolina Attorney General’s Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov
- **Oregon:** You are advised to report any suspected identity theft to law enforcement, FTC, and Oregon Attorney General. 1162 Court Street, NE, OR 97301, <http://www.doj.state.or.us> 503-378-6002
- **Rhode Island:** You may contact and obtain information from Rhode Island Attorney General Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.
- **South Carolina:** South Carolina Department of Consumer Affairs may be reached at 293 Greystone Blvd., Ste. 400, Columbia, SC 29210, www.consumer.sc.gov, 800-922-1594.
- **Vermont:** If you do not have Internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General’s Office at 802-656-3183 (800-649-2424 toll free in Vermont only).