David S. Kantrowitz
617.570.1254
DKantrowitz@goodwinprocter.com

Godwin Procter LLP
100 Northern Avenue
Boston, MA 02210

goodwinlaw.com
+1 617 570 1000

April 2, 2019

VIA EMAIL

Office of the Attorney General
State of Washington
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
SecurityBreach@atg.wa.gov

Re: **Notice of Data Security Incident**

Dear Sir/Madam:

We write on behalf of New Bit Ventures Ltd., the owner of Coinmama.com ("Coinmama"), to notify you of a data security incident that Coinmama recently experienced. Coinmama is a cryptocurrency sales platform. On February 17, 2019, Coinmama discovered that an unauthorized party acquired data associated with Coinmama user accounts in December 2018. Coinmama had first detected unauthorized activity on its platform in December 2018; initially, Coinmama believed the activity was limited to financial fraud not involving personal information. In February 2019, with the assistance of outside experts, Coinmama became aware of new evidence showing that the unauthorized activity extended to the acquisition of certain user information.

Coinmama's review found that the personal information of approximately 1,221 Washington residents was acquired by unauthorized parties. The information consists of that information Coinmama collects from users as part of its know your customer (KYC) procedures, and can include name, mailing address, email address, date of birth, and government-issued identification card information (sometimes including photocopies of identification cards). Social security numbers and credit/debit card numbers were not accessed in this incident. Coinmama notified impacted consumers during the period of February 20-22, 2019. A copy of Coinmama's notification is attached to this letter.

Coinmama takes this incident very seriously. Since the incident occurred, Coinmama has

- Shut down the unauthorized access;
- Reset passwords for all users;
- Established a dedicated support team to answer any customer questions; and
- Increased the monitoring of its computer networks.

As of the date of this letter, Coinmama is not aware of any Washington resident having suffered identity theft as a result of the incident. Coinmama continues to review its information security processes and procedures to help guard against such attacks in the future.

Thank you for your attention to this matter.

Respectfully Submitted,

David S. Kantrowitz

David S. Kantrowitz

Enclosure

APPENDIX 1 – Users notification from Feb 20, 2019

Coinmama

Dear customer,

On Sunday, February 17, we learned that an unauthorized party acquired data associated with 1.4 million Coinmama accounts. This information follows our internal investigation into a large breach that has affected 30 companies and 841 million users.

We're taking this incident extremely seriously, and want to give an overview of what it means for you, as well as the immediate actions we're taking to protect your security.

What happened
In order to sell cryptocurrency, we are required by regulation to collect certain personal information from our customers, including your name, address, email, gender and ID number. From some of our customers we are also required to collect images and copies of documents, including government issued IDs. **We do not store or record any credit card information, nor do we hold any customer funds.**

On February 17, during an ongoing investigation of a financial fraud incident that occurred in December 2018, we found evidence that an unauthorized party acquired data of our customers, including their personal information as mentioned above.

As of February 20, 2019, there has been no evidence of this information being used by perpetrators.

What we are doing
In light of this new evidence, we immediately expanded our investigation efforts, working closely with several leading security firms to determine the scope of the incident.

Second, we are devoting all resources necessary to accelerate the ongoing security enhancements to our systems. We are working diligently to protect your privacy, including:

- **Email notification**. We began sending emails on a rolling basis on February 15, 2019 to affected customers.
- **Password reset**. Since February 15, we started expiring the passwords of customers' accounts. We recommend that you set a new password, and change it on any other service using the same credentials (email and password).
- **Law enforcement**. We have reported this incident to law enforcement authorities and will continue to support their investigation.
- **Data protection authorities**. We are notifying the applicable regulatory authorities of this matter.
- **Monitoring**. We are taking additional measures to monitor any suspicious activity relating to our customers' accounts.

Third, we have also established a dedicated support team to answer your questions 7 days a week. If you have questions about this incident, reply to this email. You can also contact our designated DPO, Yaki Oliel, at dpo@coinmama.com. For other support issues, contact support@coinmama.com. We may experience high volume initially, and appreciate your patience.

What you can do
Cyber crime is a growing threat that affects billions of people worldwide and presents a daily battle

for companies, across all industries. Below are some additional steps you can take to protect your privacy online:

- Be vigilant against third parties attempting to gather information by deception (commonly known as "phishing"), such as suspicious emails or links to fake websites.
- Use strong passwords and do not use the same passwords for multiple accounts (for best practices about creating secure passwords, click here).
- Make a habit of reviewing your accounts for suspicious activities from time to time.
- If you believe you are the victim of identity theft or that your personal data has been misused, immediately contact your national data protection authority or local law enforcement.

If you are a resident of the United States: given the applicable regulations that apply in each state, click here to learn more about actions you can take.

We will continue to update everyone as our investigation progresses in this blog post, and address commonly asked questions in our dedicated FAQ.

I want to personally apologize for the distress this news may cause, and thank you for your continued support and understanding during these trying times. Your loyalty is truly appreciated, and we will work harder than ever to keep it.

Sincerely,
Nimi

Nimi Gruber

CEO & Co-Founder

Coinmama Support

Search Coinmama Support

Articles in this section

Protect yourself against identity theft

Nathan
Updated 22 days ago

Fraud and Identity theft

Please keep in mind that the below information is relevant for US citizens.

It is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- **Equifax**, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- **Experian**, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- **TransUnion**, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

If you are a resident of Connecticut, Maryland, Massachusetts, North Carolina, or Rhode Island:	You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, www.ct.gov/ag, 1-860-808-5318 Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023 or 1-410-576-6300 Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, www.mass.gov/ago/contact-us.html, 1-617-727-8400 North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400 or 1-877-566-7226 Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 1-401-274-4400
If you are a resident of Massachusetts or Rhode Island	Note that pursuant to Massachusetts or 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.
If you are a resident of West Virginia	Note that you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com

TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com

Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior 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, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity 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 one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list of FCRA rights includes

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.

- Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited. You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.