



COWAN,
DeBAETS,
ABRAHAMS &
SHEPPARD LLP

41 MADISON AVENUE
NEW YORK, NY 10010
T: 212 974 7474
F: 212 974 8474
www.cdas.com

JOSHUA B. SESSLER
212-974-7474
JSESSLER@CDAS.COM

July 18, 2022

VIA EMAIL (Idtheft@oag.state.md.us)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Security Incident

Dear Attorney General:

Pursuant to Md. Code Com. Law § 14-3501 et seq., we are writing to notify you of a data security incident involving six (6) Maryland residents.

This law firm represents Gelt Finance, Inc. ("Gelt"), an online savings account alternative through which users earn passive income on funds.

Gelt detected unusual activity on one of its servers on July 7, 2022 that impacted certain of its information technology systems. It immediately initiated response and containment protocols, shifting all traffic to isolated backup servers and rotating all third-party API keys. Gelt is based on a non-custodial system, meaning user funds were not at risk (third parties, including Gelt, cannot access user funds; only the user can, using a private key).

Gelt also engaged a leading cyber security and forensics firm to conduct a full investigation of the incident. Thus far, no conclusive signs of data exfiltration have been found. However, if such exfiltration is found to have occurred, the following personal information could have potentially been affected:

- Email used to sign up to Gelt
- Salted Password Hash
- User legal name
- Bank Name
- Deposit and withdrawal history (with respect to Gelt accounts)
- Driver's license or passport picture
- Bank statement used for account verification

Gelt will be sending the attached notice to the six (6) Maryland residents who were potentially impacted by the security incident. As stated in the notice, Gelt is suggesting that users change their Gelt passwords and offering a free 2-year enrollment in a privacy and identity protection plan with IDX, a leader in digital privacy and identity protection, including 24 months of Single Bureau Credit Monitoring services and up to \$1,000,000 insurance reimbursement policy. In addition, Gelt has shut down all potentially

JEAN ALBERT
JASON K. BERGER
FREDERICK P. BIMBLER
SUSAN H. BODINE
ANDREA F. CANNISTRACI
CAITLIN DiMOTTA ■ □ ♣
ROBERT J. EPSTEIN
BRIANA HILL ■
DOUGLAS P. JACOBS*
BENJAMIN JAFFE
ELLIS B. LEVINE
SARAH C. ODENKIRK † ♦ □ ♣
SIMON N. PULMAN* ○
JOSHUA B. SESSLER
J. STEPHEN SHEPPARD ♦
SCOTT J. SHOLDER*
KENNETH N. SWEZEY †
NANCY E. WOLFF ● * †

ELIZABETH ALTMAN
POONEH AMINIAN ■
CECE COLE
JOSHUA M. GREENBERG
MATTHEW KLEIN
SCOTT W. RESNICK
DANIEL SHEERIN ■
ARIANA SARFARAZI
AMY STEIN
ALEX STOLLS
KATHERINE WILCOX

COUNSEL:
BENJAMIN HALPERIN
LYNNETTE SANTIN-LERNER

SPECIAL COUNSEL:
ALEX GIGANTE

TIMOTHY J. DeBAETS
(1949-2020)
PHILIP M. COWAN
(1943-2001)
HOWARD ABRAHAMS
(1945-1996)

■ ADMITTED IN CA
† ALSO ADMITTED IN CA
♦ ALSO ADMITTED IN DC
○ ALSO ADMITTED IN GA
* ALSO ADMITTED IN NJ
● ALSO ADMITTED IN PA
□ ALSO ADMITTED IN WA
♣ ALSO ADMITTED IN OR
♠ ALSO ADMITTED IN NM

BEVERLY HILLS OFFICE:
9454 WILSHIRE BLVD., SUITE 901
BEVERLY HILLS, CA 90212
T: 310.340.6334



contaminated servers after deploying the backups. It installed SentinelOne monitoring software, reset all passwords and rotated access keys, leveraged all available data center native security services, and conducted a thorough forensic investigation and root cause analysis. Uptime was 100% during the incident, and deposits and withdrawals continued to be enacted without issue.

Please feel free to contact me should you require any further information.

Sincerely yours,

A handwritten signature in black ink, appearing to read 'Josh Sessler'.

Joshua Sessler

User Notices

Sent via email 7/12/22

From: Support at Gelt

Subject: User Notice

Dear User,

We have detected unusual activity on one of our servers. Our response protocols were immediately initiated, shifting all traffic to isolated backup servers and rotating all third-party API keys.

Gelt is non-custodial by design, meaning user funds are not at risk (third parties, including Gelt, cannot access your funds; only you can, using your private key). Withdrawals for active depositors through the Gelt interface are uninterrupted and are always possible directly from the blockchain, independently of our company or product (see [guide](#)).

We have also engaged a leading cyber security and forensics firm to conduct a full investigation of the incident and of our infrastructure. We are diligently working with them to assess the situation and to determine whether any user or company data has been impacted.

We will update you as soon as a final assessment has been made, typically within 2-4 business days.

Please be aware that our team will never ask for your Gelt or any other passwords. If you do receive suspicious communication from someone you believe is impersonating Gelt, please reach out to our customer success team on support@gelt.finance or on our live chat on [gelt.finance](#).

Sent via email 7/18/22

From: Support at Gelt

Subject: User notice follow-up

Dear User,

As a follow-up to the notice we sent to you on Monday, the forensics team we engaged has confirmed signs of unauthorized access to the infrastructure that was taken offline. The new isolated infrastructure shows no signs of unusual activity and continues to be continuously monitored.

Gelt is non-custodial by design, meaning user funds are not at risk (third parties, including Gelt, cannot access your funds; only you can, using your private key). Withdrawals through the Gelt interface are uninterrupted and are always possible directly from the blockchain, independently of our company or product (see [guide](#)).

We have also confirmed that no conclusive signs of data exfiltration have been found thus far. However, the most cautious approach is to assume data could have been compromised. In an abundance of caution, and while the forensic investigation continues, our records show that data from the following fields on your account could potentially be affected:

- Email used to sign up to Gelt
- Salted Password Hash
- User legal name

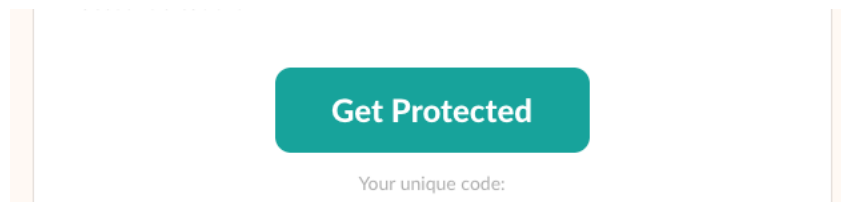
- Bank Name
- Deposit and withdrawal history (with respect to Gelt accounts)
- Driver's license or passport picture
- Bank statement used for account verification

We will continue updating you as we gain more information. In the meantime, we highly recommend you take the following steps to protect yourself:

1. Change your Gelt password and ensure your previous password was not used with any other service. Widely used password managers such as 1Password or LastPass make this easy.

2. Enroll in IDX's privacy and identity protection plan to proactively protect your privacy and identity across all the services you use. We have partnered with IDX, the leader in digital privacy and identity protection, to offer two full years of protection to users who wish to enroll, cost-free. This includes 24 months of Single Bureau Credit Monitoring services and up to \$1,000,000 insurance reimbursement policy.

Read more about IDX here and follow this link to get started: <https://app.idx.us/account-creation/protect> using your unique code: {{insert code "default="}} upon account creation.



When the investigation is concluded, we will follow up with a summary of the event. Please be aware that our team will never ask for your Gelt or any other password. If you do receive suspicious communication from someone who you believe is impersonating Gelt, please reach out to our customer success team on support@gelt.finance or on our live chat on gelt.finance.