GSPlatformCo Inc.
2810 N Church St
PMB 512358
Wilmington, Delaware, 19802-4447 US
+1 (913) 406-5757
matilda@globalshop.co

January 8, 2026

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504

Dear Attorney General,

Notification of Data Breach Pursuant to Wash. Rev. Code §§ 19.255.005 – 19.255.040
Pursuant to Wash. Rev. Code §§ 19.255.005 – 19.255.040, GSPlatformCo Inc. hereby submits this notice to inform the Washington Attorney General of a data security incident that may have involved the unauthorized access to certain personal information of Washington residents.

The relevant details are below:

1. **Reporting Entity**
   GSPlatformCo Inc. operates an e-commerce platform that facilitates the sale of physical products sourced from its vendor network to customers registered with the Delaware laws, with EIN 39-3224417 and headquartered in Delaware. We are submitting this notification and in compliance with applicable Delaware law on data breach notification reporting requirements.

2. **Summary of the Incident**

GSPlatformCo Inc.

2810 N Church St, PMB 512358 - Wilmington, Delaware, 19802-4447 US

On 22 October 2025, GSPlatformCo Inc., a New York–based company, acquired ANKA, an Ivorian e-commerce platform, through bankruptcy proceedings before a French court following the insolvency of ANKA's parent entity. The transaction comprised the acquisition of specified Intellectual Property (IP) assets, two subsidiaries, and one operational branch.

Prior to the acquisition, ANKA's technical infrastructure relied on a combination of cloud-service providers to support its e-commerce, search and analytics functions. In particular, ANKA utilised DigitalOcean's low-cost and rapidly deployable server environment to host certain search and analytics services, enabling customers to browse products efficiently and allowing sellers to track performance metrics while maintaining relatively low infrastructure costs.

During a migration from DigitalOcean to Hetzner Online GmbH ("Hetzner"), a German-based cloud infrastructure provider in May, an oversight occurred. An Elasticsearch index on DigitalOcean, containing a snapshot from April 2025, was misconfigured leaving this dataset publicly accessible. An unauthorised third party discovered the misconfiguration and downloaded the snapshot. The exposed dataset was approximately seven months old and separate from the company's core production database, so no passwords, payment data or recent orders were compromised. Nevertheless, the index contained unencrypted customer profile information. As soon as GSPlatformCo Inc. learned of the exposure, it isolated the DigitalOcean environment, it removed all personal data from Elasticsearch indexing, stopped relying on it for admin dashboards, switched to querying directly from the secure PostgreSQL database and audited all Elasticsearch indices.

The business functions once supported by the DigitalOcean environment are now running on the new Hetzner platform. The migration has allowed GSPlatformCo Inc. to implement better organisational and technical controls such as private VPC access, firewalls, encryption at rest, pseudonymisation of personal identifiers and stricter access controls. Before going live, the security team commissioned an independent penetration test and vulnerability scan of the Hetzner deployment. The assessment confirmed that the configuration was robust and that no publicly accessible endpoints or misconfigured databases remained. GSPlatformCo Inc. continues to monitor the new environment and believes it is now secure and resilient against similar breaches.

3. **Timing of the incident**

   Based on our investigations, the incident is believed to have occurred between approximately May 2025 and discovered on November 22nd, 2025. Investigation remains ongoing and these dates may be refined as additional information becomes available.

4. **Systems Involved**

   From our investigations, the following organizational systems were involved in the breach:

   - ElasticSearch server hosted on DigitalOcean

5. **Categories of Personal Data Involved**

   The potentially affected data may have included the following categories of personal information, as defined under Washington law:

   - First and last name
   - Gender
   - Birth date
   - Phone number
   - Email address
   - Delivery address
   - Account status and balance
   - Sales and purchases list
   - Last sign-in date

6. **Affected Data Subjects**

   Based on our investigations, we estimate that approximately 798 residents may have been affected by this incident.

7. **Risk Assessment and Impact Analysis**

   GSPlatformCo Inc. conducted a data breach impact assessment to evaluate the potential impact of the incident on the rights and freedoms of affected individuals. Based on the nature of the incident, the types of personal information involved, and the foreseeable

consequences, the assessment concluded that the incident presents a low risk to affected individuals. A copy of the data breach impact assessment is attached to this letter.
In addition, we have implemented corrective and remediation measures to mitigate any potential effects of the incident and to reduce the likelihood of future occurrences.

8. **Corrective Actions and Remediation Measures**

At this time, we have taken the following corrective and remediation actions:

- Removed all personal data (emails, names, phone numbers) from Elasticsearch indexing.
- Stopped relying on Elasticsearch for admin dashboards, switching to querying directly from our secure PostgreSQL database.
- Audited all Elasticsearch indices to ensure only non-sensitive fields are ever indexed.
- Secured our current Hetzner Elasticsearch cluster with strict access controls, including private VPC access and firewalls, to prevent any public exposure.

9. Consumer Notification

In compliance with Wash. Rev. Code §§ 19.255.005 – 19.255.040, we will provide a written notice to the affected Washington residents. A sample copy of the consumer notification letter is enclosed to this letter.

10. Reason for Delayed Notification

Upon detection of suspicious activity, our incident response team immediately initiated corrective and remedial actions to secure the affected systems and limit any potential impact on data subjects. In parallel, post-incident reviews were conducted to determine whether personal data had been compromised, to identify the categories of personal data involved, and to assess the potential impact of the incident on the rights and freedoms of affected data subjects.
Given the cross-jurisdictional nature of the systems and data involved, additional time was required to assess the incident under the applicable data protection laws in each relevant jurisdiction and to determine the corresponding regulatory obligations, including breach notification requirements.
On the advice of internal legal and compliance teams, the organisation proceeded with a comprehensive investigation to establish the full scope of the incident and the extent of

any actual or potential harm. While certain data protection frameworks permit phased or delayed notification in specific circumstances, many require that notifications be based on verified information and contain sufficient detail to enable regulators and affected individuals to meaningfully assess the nature and potential impact of the incident.
Notification was therefore deferred to allow completion of a full investigation, including confirmation of the affected data sets, identification of impacted data subjects, assessment of residual risks, and implementation of post-incident monitoring. This approach ensures that the information provided to your office is accurate, complete, and meaningful, rather than preliminary or speculative.

11. Contact Information

Should your office require additional information regarding this matter, please contact:

Matilda Ceesay
Founder & CEO
+1 (913) 406-5757
matilda@globalshop.co

Our Company GSPlatformCo Inc. remains committed to protecting personal information and to cooperating fully with the Washington Attorney General's Office.
We will provide supplemental information should material facts change as the investigation progresses.

Sincerely,

Matilda Ceesay
Founder & CEO
GSPlatformCo Inc.

Subject: ANKA Security Incident

Transparency is important to us, so we want to inform you about a recent data exposure incident that affected a portion of our user data. **Please note this was not a breach of ANKA's core database.** No passwords, payment card data, login access tokens, or sensitive files were compromised or exposed.

What happened

We recently detected unauthorized access to data hosted by one of the systems we used to store customer information. This incident did not involve login credentials, passwords, payment card details, or other highly sensitive data. We also confirmed that the related data is a snapshot from April 2025 (a dataset approximately 7 months old), confirming our current environment is secure.

What this means for you

The categories of data contained in the affected system include basic profile details (such as name, contact information, and demographic data), account status, and basic transaction history. No authentication tokens or financial information were involved

Our response

Upon discovery, we immediately launched a security investigation and fully hardened our environment against any additional exposure. We have also notified the relevant data protection authorities, as required by law, and are enhancing our security controls to prevent a recurrence

Trust, security, and privacy are foundational to our products, our organization, and our mission. We are committed to transparency and are notifying all potentially impacted customers.

Recommended Actions

The information that may have been exposed could be used as part of phishing or social engineering attacks against you. Since names and email addresses were included, we encourage you to remain vigilant for credible-looking phishing attempts or spam.

As a reminder:

- Treat unexpected emails or messages with caution, especially if they include links or attachments.
- ANKA will never request your password, payment card details, or verification codes through email, text, or chat.
- For your security, we always recommend using a strong, unique password for your ANKA account.

We regret any concern this may cause and remain committed to protecting your data.

Please contact the ANKA Security Team at security@anka.africa if you have any questions or need our support.
Sincerely,

Sincerely,

Matilda Ceesay

ANKA CEO