SUBJECT: Data Breach Notification

Report Type: Initial complete Report

Reporting Entity (and data controller):

Genvey 1A N.V. Curaçao Corporate Entity

Werfstraat 6F Willemstad

+599 9 788 9958

webmaster@genvey.com

Reason for report

We consider the incident meets the threshold to report

About the breach

Please describe what happened

Genvey 1A N.V. is a company registered in Curaçao.

Genvey is the provider of online wallets and app functionality for the purposes of promoting the Electroneum cryptocurrency (ETN).

Genvey is not established in, or operating from New Hampshire and does not specifically market its services to New Hampshire users of Electroneum or provide services within New Hampshire. However, Genvey's services are globally available. This is a precautionary disclosure, this is not confirmation that we are conducting business in New Hampshire or anywhere else in the United States (as we are not).

An external hacker claims to have gained access to 2 accounts of individuals resident in New Hampshire by exploiting a vulnerability in third party supplier software. Using that access the hacker has undertaken a number of transactions in an attempt to transfer ETN out of their accounts. As part of this attempt, the hacker claims to have had peripheral access to certain databases which include user information although no irrefutable evidence of this has been found during our ongoing investigations.

However, our analysis and the information available from AWS (our storage providers) so far initially suggested that the primary focus of this attack was theft of the ETN cryptocurrency gaining access to ETN accounts for financial gain.

New communications from the hacker have alluded to copying of wider datasets and extortion to prevent release of the information – which the hackers make claims to have obtained, including: names, ETN balances, ETN Online Wallet addresses, encrypted (one way) passwords, PINs, email addresses, FACEBOOK/GOOGLE/APPLE login emails (if used), mobile phone numbers, recovery email addresses, total transactions, country, timezone, dates of access and potentially other information including the KYC or other information uploaded.

Please describe how the incident occurred

A vulnerability in third party supplier software was exploited to gain access to the system.

Existing Security Measures

Automated alerts notifying of unauthorised activity was how we detected this intrusion.

Data was encrypted on **KMS Amazon Web Services S3 bucket AES encryption**

How did the organisation discover the breach

We initially became aware when certain users reported automated alerts notifying them of activity in their online ETN wallets which they had not authorised. Subsequently we investigated and were able to suspend the system within 30 minutes of the breach being confirmed.

What preventative measures did you have in place

Automated systems notifications as outlined above.

Was the breach caused by a cyber incident?

Yes

When did the breach happen?

Date: 23/08/2021 is the date that unauthorised access to the AWS account was first gained. Unauthorised Account activity commenced 26/08/2021 at 11:59

When did you discover the breach?

Date: 28/08/2021 14:06 following user queries related to automatic notifications of transactions which were unauthorised. The system was suspended at 14:35.

Categories of personal data included in the breach (tick all that apply)

Basic personal identifiers, eg name, contact details

Identification data, eg usernames, passwords

Official documents, eg driving licences

Economic and financial data, eg credit card numbers, bank details

Number of personal data records concerned?

2 accounts of individuals resident in New Hampshire.

How many data subjects could be affected?

2 accounts of individuals resident in New Hampshire

Categories of data subjects affected (tick all that apply)

Users

Potential consequences of the breach

Certain individuals whose accounts were compromised had ETN transferred out of their accounts. We have replaced all such ETN and so those individual accounts' correct balance has been restored.

In relation to the wider database, while there is a threat that the information included there could be used for identity theft or other cybercrime, there is no evidence in the forensic analysis which is ongoing that this has currently been executed.

Is the personal data breach likely to result in a high risk to data subjects?

The information that is alleged to have been copied could be used for identity theft or other cybercrime.

We have mitigated the position for all most seriously affected data subjects by personal direct communication informing them of the data breach and advising them to maintain vigilance and implement enhanced security measures. This message has also been articulated to the whole of the wider ETN Community generally and repeating the messages about maintaining increased vigilance and implementing enhanced security measures too.

Please give details

Please see details above regarding the mitigating actions taken following the breach to protect ETN users.

(Cyber incidents only) Recovery time

We have implemented new security measures and protocols and are implementing further protective technical measures as part of an impending blockchain rollout.

If there has been a delay in reporting this breach, please explain why

We were gathering full information in relation to the breach and taking immediate steps to mitigate its impact by:

(1) informing affected data subjects of the security breach; and

(2) preventing any further issues by implementing new security protocols; and

(3) preserving and gathering forensic evidence for law enforcement; and

(4) Negotiating with the Hackers to dissuade them from releasing data.

Taking action

Describe the actions you have taken, or propose to take, as a result of the breach

All affected data subjects have been informed of the security breach.

We have replaced all ETN transferred out of individual affected accounts as a result of the breach and so those individual accounts' correct balance has been restored.

New security protocols have been implemented and fresh staff training has been initiated for increased awareness throughout the business.

Have you taken actions to contain the breach? Please describe these remedial actions

1. The system was suspended within 30 minutes of the breach being confirmed.

2. New security protocols have been implemented.

3. Fresh staff training has been initiated.

4. Further protective technical measures are being implemented as part of an impending blockchain rollout.

Please outline any steps you are taking to prevent a recurrence, and when you expect they will be completed

New security protocols have been implemented and fresh staff training has been initiated for increased awareness throughout the business. Further protective technical measures are being implemented as part of an impending blockchain rollout.

Have you told data subjects about the breach?

Yes – emailed (see end of document for email details).

Have you told, or are you planning to tell any other organisations about the breach?

Yes

If you answered yes, please specify

Data protection supervisory authorities in EU member states and other jurisdictions for those other individuals whose information has been compromised.

About you

Organisation (data controller) name

Genvey 1A N.V.

Registration number

N/A

If not registered, please give exemption reason

We are not based or established in the New Hampshire or anywhere else in the United States.

Business sector

Crypto Currency

ETN Community wide notification:

We can confirm that following on from our recent communications regarding anomalous network activity on 10 September 2021, we have now been contacted by the alleged unauthorised actor/actors who claim responsibility for this criminal intrusion (via a vulnerability in a third party application) and a potentially serious security breach affecting less than 0.2% of our users, who have already been contacted by us directly.

These issues occurred due to a criminal cyber-attack breaching security via a third-party software vendor's application that resulted in unauthorised access to the system. In addition to attempted theft of ETN, the hackers make claims to have obtained names, ETN balances, ETN Online Wallet addresses, encrypted (one way) passwords, PINs, email addresses, FACEBOOK/GOOGLE/APPLE login emails (if used), mobile phone numbers, recovery email addresses, total transactions, country, timezone, dates of access and potentially other information including the KYC or other information uploaded.

We are working diligently to verify the full extent of these claims, however, we feel it is prudent for us to alert you of our concerns sooner rather than later.

We have already communicated directly with the relevant ETN Users.

Please be assured that no ETN User Online Wallet balances have been adversely impacted by this criminal intrusion.

Please continue to follow all previous guidance regarding changing your unique password, PIN and consider cold storage of your ETN. ETN-Network has provided guidance to ETN users on how to safely store their ETN in an offline (cold storage) wallet in a manner which is not vulnerable to cyber-attacks. These are also known as paper wallets. It is recommended that you do not store large amounts of cryptocurrency on ANY live system (such as leaving in an exchange wallet, or any type of custodial wallet). Please also familiarise yourself with our Best Practice guidance.

Please continue to remain vigilant for phishing emails - it is always best to verify the legitimacy of any email you receive. Never attempt to log in unless you are on my.electroneum.com or the official ETN-App.

Amongst all this activity, please know that our overriding objective is to protect the ETN Community at all times.

Any further updates will be made on the ETN-Network Community Forum.

We will continue to work with all regulatory authorities, law enforcement and other specialist security providers to protect the ETN-Network Community.

We sincerely apologise for the inconvenience and consternation caused and assure you that keeping the ETN community safe and secure is paramount to all we do.

Genvey 1A N.V. Curaçao Corporate Entity

Digitally signed by Genvey 1A N.V. Curaçao Corporate Entity
Date: 2021.09.20 20:37:57 -04'00'