ISS GLOBAL / INSIGHT REPORT

The Maileva data breach

22 million recipients and the company behind their mail

REPORTING / REVIEW WINDOW

Mid-September to 17 November 2026. Reporting reviewed through 14:51 GMT (15:51 CET) on 17 November.

ISSUE DATE

2026-11-17

Hospitals and other organisations can outsource the letters they send. Their recipients may never deal directly with the provider. La Poste says a September cyberattack on Maileva exposed the names and postal addresses of 22 million people.

A hospital’s notice illustrates why a mailing breach can have different consequences depending on who sent the letter and what information it contained. [1] [2] [3] [4]

01 / EXECUTIVE SUMMARY

What happened and its threat significance

COUNTRY

France

WHERE

France. Maileva is a subsidiary of Docaposte, part of La Poste Groupe. Client organisations disclosed impacts on their own correspondence. [1] [3] [4]

WHEN

Intrusion in mid-September 2026. Public confirmation of the overall scale on 14 and 15 November. Reporting reviewed through 17 November. [1] [2] [7]

What happened

La Poste said a cyberattack on its business-mail provider Maileva exposed names and postal addresses for 22 million recipients. It said the CNIL was notified and a complaint was filed. The Paris prosecutor's office confirmed a specialist police investigation to AFP. [1] [2] [6]

Threat significance

The identity data creates scope for impersonation and payment scams. Notices from individual senders show why the risks can vary by mailing and may extend to sensitive information. [3] [4] [8]

> EXECUTIVE JUDGEMENT
>
> The useful question for recipients is which sender and which mailing were affected. For investigators, identity fields, mailing metadata, document access and subsequent fraud require distinct evidence. [1] [3] [4] [5] [8]

02 / CHRONOLOGY

From September intrusion to November disclosure

DATE	DEVELOPMENT	WHAT THE SOURCE ESTABLISHES
Mid-September	Attack on Maileva	La Poste dates the intrusion to mid-September. It says it began informing affected client organisations within days of identifying the incident. [1]
9 October	Occupational health notice	Santé au travail en Cornouaille posts a notice describing exposure of information used to track mail, with additional fields specific to its context. [3]
28 October	Hôpital Foch learns of possible document access	The hospital dates its own awareness of possible access to some payment reminders to 28 October. A specialist outlet dates the hospital's notice to 6 November. [4] [5]
14–15 November	Scale disclosed publicly	La Poste confirms the figure to AFP on 14 November and publishes a statement on 15 November. The Paris prosecutor's office confirms the assignment of the investigation to a specialist unit. [1] [2] [6]
16–17 November	Follow-up reporting	Trade reporting clarifies the distinction between the group's disclosure and the notices of individual clients. [7] [13]

The September attack, a sender's later awareness and the November public disclosure are separate dates. The public record reviewed does not establish the exact date of notification to the CNIL or when every recipient was told. [1] [3] [4] [7] [9]

03 / HOW THE EXPOSURE SPREAD

What was exposed, and for whom

SCOPE	WHAT IS SUPPORTED	LIMIT
22 million recipients	La Poste reports disclosure of given names, surnames and postal addresses.	The estimate counts people reported affected. It is not a count of stolen documents, lost funds or subsequent fraud. The public statement gives no counting method. [1] [2]
Mail tracking at one client	The occupational health service says sender details, recipient title or gender, and file names could also have been involved.	The notice covers that service. It says it has no evidence that its own document contents were accessed or extracted. [3]
Certain Hôpital Foch letters	The hospital says some payment reminders may have been viewed. They included invoice numbers, dates of care and amounts due. The hospital named Kiwee as an intermediary.	The notice is specific to the relevant letters and does not establish that the hospital's own network was breached or that all Maileva documents were accessible. [4] [5]

The practical difference

A name and postal address can support a convincing impersonation attempt. A sender or document context may add sensitivity, particularly where it reveals contact with a healthcare organisation. The available sources establish exposure or possible access. They do not measure fraud that followed. [1] [3] [4] [8]

04 / A DOCUMENTED CASE

A hospital letter with several organisations behind it



Plate 1. Hôpital Foch in Suresnes, photographed by Celette on 23 June 2018. Archival context for a sender that issued a notice. Image resized. CC BY-SA 4.0 [4] [12]

SENDER	INTERMEDIARY	MAILING PROVIDER	RECIPIENT
Hôpital Foch	Kiwee	Maileva	Patient receiving a relevant reminder [4] [5]

The hospital's notice concerns reminders in the 9–23 September period. This chain describes that case only. An intermediary can leave people recognising the hospital that contacted them while having no direct relationship with the business that processed the mail. [4] [5]

When a sender's notice mentions letters or possible document access, the document type, date range, exposed fields and affected cohort matter more than the national headline number. [1] [3] [4]

05 / PUBLIC AND BUSINESS IMPACT

Who bears the cost of a breach like this?

For recipients

For an unexpected request involving money or personal information, verify it with the sender using contact details you already trust or obtain from its official website. If you have already sent money or banking details in response to a suspicious request, contact your bank promptly and preserve the correspondence. [4] [8]

For organisations

Likely costs include investigating the scope, identifying affected mailings, handling recipient enquiries and coordinating consistent notices across suppliers. The reviewed sources give no reliable financial estimate for Maileva. Under the GDPR framework described by the CNIL, roles and risk determine who must notify the regulator and affected people. The public statement alone cannot establish which notification duties applied or whether they were fulfilled. [1] [3] [4] [9]

Why the comparison with financial theft matters

On 12 November, the US Department of Justice announced court-authorised seizure and restraint of more than $1.2 billion in cryptocurrency stolen from Binance. On 4 November, Crédit Mutuel Arkéa said its own funds were affected by fraudulent transactions and that it was still assessing the amount. Maileva's 22 million is a count of people. In a data breach, restricting further access cannot recall information that has already escaped. [1] [10] [11]

The comparison is about consequences and recovery. The reviewed sources establish no operational connection between these cases. [1] [10] [11]

06 / EVIDENCE AUDIT

What would change the assessment

QUESTION	BEST NEXT EVIDENCE
How was the 22 million figure produced?	A dated scope statement showing how recipients were counted and deduplicated, and any revised total. [1]
Where was document access possible?	A sender-level reconciliation of notices, the fields involved and the relevant date ranges, distinguishing possible access from confirmed disclosure. [3] [4] [5]
Were the data later used in fraud?	Corroborated victim reports or official case findings linking a specific scam to this breach while protecting personal data. [6] [8]

Confidence is high in the 22 million figure as a published La Poste disclosure and in the existence of client-specific notices. The exact dataset, complete recipient coverage, actor identity and attributable losses remain unestablished in the reviewed public record. [1] [3] [4] [6] [7]

SOURCE REGISTER

Sources 01–05

Source families and access limits are recorded below. Repetition of a statement is not independent proof.

01 Cyberattaque de Maileva, ce qu’il faut savoir

La Poste Groupe · 15 Nov 2026

Family: Primary group statement · Confirms the 22 million figure and identifies affected recipient fields.

https://www.lapostegroupe.com/fr/actualite/cyberattaque-de-maileva-ce-quil-faut-savoir

02 Une filiale de La Poste victime d’un vol de données massif, 22 millions de personnes concernées

AFP / **TV5MONDE** · 14 Nov 2026

Family: Wire report with company confirmation · Company account of scope carried by AFP. Company claims share the source family in [1].

https://information.tv5monde.com/economie/une-filiale-de-la-poste-victime-dun-vol-de-donnees-massif-22-millions-de-personnes-concernees-2845846

03 Incident de sécurité ayant affecté l’un de nos prestataires, la société MAILEVA

Santé au travail en Cornouaille · 9 Oct 2026

Family: Primary client notice · Sender-specific tracking data and qualifications concerning its own documents.

https://www.stc-quimper.org/type-dactualite/vie-de-lassociation-13

04 Violations de données Maileva-Kiwicare

Hôpital Foch · 6 Nov 2026, reported date

Family: Primary client notice, indexed excerpts · Indexed notice provided event detail. Direct page was unavailable during review. Read alongside [5].

https://www.hopital-foch.com/actualites/violations-de-donnees-maileva-kiwicare/

05 Docaposte confirme le vol des adresses de 22 millions de Français après une cyberattaque chez cette filiale de La Poste

Cyberattaque.org · Updated 12 Nov 2026

Family: Specialist reporting and sender notices · Reports the hospital’s notice and dates it to 6 November. Article records operator response.

https://www.cyberattaque.org/maileva-docaposte-la-poste-cyberattaque/

SOURCE REGISTER

Sources 06–09

Source families and access limits are recorded below. Repetition of a statement is not independent proof.

06 Cyberattaque d’une filiale de La Poste : la Brigade cybercriminalité enquête

AFP / **Zonebourse** · 15 Nov 2026

Family: Paris prosecutor’s office via AFP · Attribution limited to the confirmation of the investigative assignment.

https://www.zonebourse.com/actualite-bourse/cyberattaque-d-une-filiale-de-la-poste-la-brigade-cybercriminalite-enquete-ce785ededc81ff21

07 Criminals attack French postal operator subsidiary, grab contact details of 22M people

The Register · 16 Nov 2026

Family: Trade reporting, operator and client statements · Reviewed for corroboration of public scope and downstream notices.

https://www.theregister.com/cyber-crime/2026/11/16/criminals-attack-french-postal-operator-subsidiary-grab-contact-details-of-22m-people/5310070

08 Violation ou fuite de données personnelles, que faire ?

Cybermalveillance.gouv.fr · Accessed 17 Nov 2026

Family: Official public guidance · General risk and protective advice.

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/que-faire-en-cas-de-fuite-de-donnees-personnelles

09 Chapitre IV – Responsable du traitement et sous-traitant

CNIL · Accessed 17 Nov 2026

Family: Data protection authority / GDPR · General framework, particularly Articles 33 and 34. No case-specific finding.

https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4

SOURCE REGISTER

Sources 10–13

Source families and access limits are recorded below. Repetition of a statement is not independent proof.

10 Justice Department Announces Actions to Disrupt North Korea’s Massive Theft of Cryptocurrency

US Department of Justice · 12 Nov 2026

Family: Primary enforcement statement · Used solely for court-authorised Binance asset action.

https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-north-koreas-massive-theft-cryptocurrency

11 Informations complémentaires suite à l’attaque dont le Crédit Mutuel Arkéa a été victime

Crédit Mutuel Arkéa · 4 Nov 2026

Family: Primary corporate statement · Used solely for bank-funds impact and preliminary loss scope.

https://www.cm-arkea.com/arkea/banque/assurances/pa_38386/fr/informations-complementaires-suite-a-l-attaque-dont-le-credit-mutuel-arkea-a-ete-victime

12 Hôpital Foch (Suresnes) 1.jpg

Celette / **Wikimedia Commons** · 23 Jun 2018

Family: Archival photograph · CC BY-SA 4.0. The caption links to the licence. Image resized without cropping.

https://commons.wikimedia.org/wiki/File:H%C3%B4pital_Foch_(Suresnes)_1.jpg

13 22 million impacted in attack on French postal subsidiary

IT Pro · 17 Nov 2026

Family: Trade follow-up · Follow-up coverage. Repetition of the operator figure is not independent verification of the count.

https://www.itpro.com/security/cyber-attacks/22-million-impacted-in-attack-on-french-postal-subsidiary