KILLSWITCH · ISSUE #15 · 16 NOV 2026

Your Newsletter Vendor Was the Database

An email-marketing supplier reported 81.3 million addresses taken or at risk (addresses, not people), and its sending address was used for phishing. Treat your mailing vendor as a data processor.

Killswitch rating: Review your mailing vendor

By Emmanuel Aigbehi Walstra

Your newsletter vendor was the database

Arara Message first reported ~3.01 million leaked addresses on 29 October [1]. By 6 November the count was 81,329,467 [4].

- Up to ~380 customer companies, an estimate still being checked [5].
- Its own sending address was used for phishing [3][5].

Addresses, not people

- 81,329,467 is email addresses with duplicates removed, not people [4].
- It includes records only "at risk" of being taken [3][5], judged from read volume [3].
- 47,044,380 came with member details; 34,285,087 were addresses only. Still being checked [4].
- Quotes and figures: our translation of Japanese filings.

03 · TIMELINE

Three filings, and the number kept growing



Arara [1][5], PayCloud filings [2][3][4], Sega [6]. All dates 2026. On 29 Oct, the order of the notice and Sega's answer is not stated.

How the count grew in eight days

1

29 Oct: ~3.01 million

One system (a shared environment). Cause: a web-server vulnerability

→

2

2 Nov: ~77 million

Plus 97 servers in customer environments, up to ~380 companies

→

3

6 Nov: 81,329,467

Plus a second cloud environment. Duplicates removed

PayCloud filings [3][4], Arara [1]. Counts are email addresses, not people, and include records only "at risk" of being taken [3][5].

05 · ABUSE

The vendor's own address sent the phishing

- 28 to 30 October: up to ~7.13 million fake card-company emails [3][5].
- Sent from **news@arara.com**, the service's own address [3].
- Sent to addresses the attacker brought in from outside [3]; not counted in the 81.3M [5].
- The service was stopped on 31 October [3].

Sega: told "no leak confirmed", then told it leaked

- 29 Oct (same day as the first notice; order not stated): Sega asks, told no leak confirmed [6].
- 3 Nov: Arara tells Sega its addresses were taken [6].
- 2,196,044 addresses; the leaked data did not include names, card data or passwords [6].
- No misuse confirmed as of 9 November [6].

07 · WHAT IT HELD

What a "newsletter vendor" was holding

1 **Address books**

Email plus, for some customers, name, sex, date of birth, phone, member number, address

2 **Mailing records**

Who was sent what: the delivery records

3 **Customer API keys**

Used to connect to the service. Now suspended

4 **Customer staff**

Names and emails of admin-screen users: still being checked

Per PayCloud filing [3], table 2. Fields vary by customer. Whether API keys or staff details were taken is not stated.

Five controls for your mailing vendor

1 Send less

Only the fields each mailing needs

2 Ask a better question

"No leak confirmed" is not "no leak"

3 Rotate what you gave them

API keys and admin passwords

4 Watch their sending address

Phishing can come from your vendor

5 Keep the exit

Your own master list; deletion on exit

Killswitch's own controls, drawn from this case [3][6] and GDPR [7].

Killswitch's own controls.

Where this lives in your frameworks

Choose and contract	A.5.19, A.5.20 · NIS2 21(2)(d), 21(3) · GDPR Art. 28 · Evidence: DPA, notification clause
Minimise	A.5.34 · GDPR Art. 5(1)(c) · Evidence: field list per mailing
Monitor	A.5.22 · NIS2 21(2)(d) · Evidence: vendor review, sending-domain watch
Respond and exit	A.5.24, A.5.26 · GDPR Art. 33, 28(3)(g) · Evidence: key rotation log, exit test

Killswitch's own mapping. Check ISO titles against your licensed copy.

ISO/IEC 27001:2022 [9] · NIS2 Art. 21 [8] · GDPR Arts. 5, 28, 33 [7]. Killswitch mapping.

10 · STILL OPEN

What we don't know yet

- The route in and start date: under investigation [3][5].
- The final count and the 380-company estimate [4][5].
- Whether API keys or staff details were taken: not stated [3].
- Misuse: none confirmed by Sega so far [6].

This week

- List every service that sends email in your name, and what it holds.
- Cut the fields the mailings do not use.
- Check the notification and exit clauses.
- Test rotating the vendor's keys and passwords.
- Keep your own master list.

Sources

[1] Arara Inc.: Information leak and service suspension due to unauthorised access to Arara Message (first notice, 29 Oct 2026, Japanese)
[2] PayCloud Holdings (TSE 4015): Unauthorised access to Arara Message, information leak and service suspension, 1st report (TDnet filing, 29 Oct 2026, Japanese)
[3] PayCloud Holdings (TSE 4015): Unauthorised access to Arara Message, information leak and service suspension, 2nd report (TDnet filing, 2 Nov 2026, Japanese)
[4] PayCloud Holdings (TSE 4015): Unauthorised access to Arara Message, information leak and service suspension, 3rd report (TDnet filing, 6 Nov 2026, Japanese)
[5] Arara Inc.: Apology and next steps regarding unauthorised access to Arara Message (6 Nov 2026, Japanese)
[6] Sega: Apology and notice on a personal-information leak caused by unauthorised access to a contractor (9 Nov 2026, Japanese)
[7] GDPR, Regulation (EU) 2016/679, Articles 5, 28 and 33 (EUR-Lex)
[8] NIS2 Directive (EU) 2022/2555, Article 21 (EUR-Lex)
[9] ISO/IEC 27001:2022 Information security management systems

Facts are from Arara's notices, PayCloud Holdings' filings of 29 October, 2 and 6 November, and Sega's notice of 9 November, as published by 10 Nov 2026. The sources are in Japanese; quotes and figures are our translation. The controls and the framework mapping are Killswitch's own.

FROM THE PUBLISHERS OF KILLSWITCH

Know what every supplier holds, and prove it

GRCOMPLIANCE

Keep a register of suppliers and the personal data each one holds, link the contract and the evidence, and map controls to ISO 27001, NIS2 and GDPR.

Try the live demo →

demo.grcompliance.com

Self-host free: github.com/Sectutor/GRCompliance-Core

SECTUTOR

Security and GRC books, training and audit kits.

sectutor.com

Emmanuel Aigbehi Walstra is a CISO who also serves as a virtual CISO (vCISO) for several organisations, with 30+ years in cybersecurity, 10,000+ people trained, and author of the CCSP Excellence books.