INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-14 06:04 UTC

Basic-Fit Breach Exposes Bank Data for 1 Million Members Across Six EU Countries

DATA BREACH | HIGH | CVSS 5.0

SCC Item ID	SCC-DBR-2026-0091
Type	Data Breach
Severity	HIGH
CVSS Base Score	5.0
Affected Products	Basic-Fit member management and visit-recording systems (Netherlands, Belgium, Luxembourg, France, Spain, Germany)
Published	2026-04-13T17:50:01
Discovery Source	Rss

Executive Summary

Basic-Fit, a major European fitness chain, confirmed a data breach affecting approximately 1 million members across the Netherlands, Belgium, Luxembourg, France, Spain, and Germany. Attackers exfiltrated names, addresses, email addresses, phone numbers, dates of birth, and bank account details from member management and visit-recording systems. The inclusion of bank account data significantly elevates financial fraud risk for affected members and triggers GDPR breach notification obligations across six EU jurisdictions.

Technical Analysis

Basic-Fit's member management and visit-recording systems were compromised, resulting in exfiltration of full PII and bank account data for approximately 1 million members. No CVE is associated; this is an organizational breach, not a disclosed software vulnerability. The initial access method and attack vector have not been publicly confirmed. Relevant CWEs: CWE-359 (Exposure of Private Personal Information to Unauthorized Actor), CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor), CWE-284 (Improper Access Control). MITRE ATT&CK techniques mapped to the breach pattern include T1005 (Data from Local System), T1114 (Email Collection), T1078 (Valid Accounts), T1567 (Exfiltration Over Web Service), T1530 (Data from Cloud Storage), T1213 (Data from Information Repositories), and T1041 (Exfiltration Over C2 Channel). Threat actor identity is unknown. No patches are applicable; organizational response focuses on access revocation, forensic investigation, and regulatory notification. Attack timeline prior to detection is unconfirmed. Sources: BleepingComputer (T2 cybersecurity news), The Record (T2 cybersecurity news); URLs require human validation for current availability.

Action Checklist

1. Containment: If your organization operates member management, fitness, or subscription-based CRM platforms with stored bank account or payment data, audit current access controls immediately. Identify and revoke any anomalous or unauthorized account sessions. Isolate affected systems from production if forensic investigation is ongoing.
2. Detection: Review authentication logs on member management and data repository systems for anomalous access patterns: bulk data reads, unusual export volumes, off-hours access, or access from unexpected IP ranges. Correlate against T1078 (Valid Accounts) indicators, look for credential use outside normal geographic or time baselines. Query SIEM for large outbound data transfers (T1041, T1567) from systems housing member PII or financial data.
3. Eradication: Reset credentials for all accounts with access to member management and visit-recording systems. Enforce MFA on all administrative and data-access accounts. Review and tighten data access permissions to least privilege. Confirm no persistent attacker footholds remain via endpoint and network forensics.
4. Recovery: Validate that data exfiltration has ceased by monitoring outbound traffic baselines. Confirm integrity of member data stores. Notify affected members per GDPR Article 34 obligations where breach poses high risk to individuals. Coordinate with legal and DPO to meet GDPR Article 33 supervisory authority notification deadline (72 hours from confirmed discovery) in each affected jurisdiction.
5. Post-Incident: Conduct a data minimization review: assess whether bank account data retention in member management systems is operationally necessary and aligned with GDPR data minimization principles (Article 5(1)(c)). Implement data-at-rest encryption for PII and financial data fields. Establish a continuous monitoring control for bulk data access anomalies. Review third-party data processor agreements for all vendors with access to member data.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to executive leadership, legal counsel, and the designated Data Protection Officer immediately upon confirmation that IBAN or bank account data was exfiltrated, as this triggers mandatory GDPR Article 33 supervisory authority notification within 72 hours across all six affected EU jurisdictions (NL, BE, LU, FR, ES, DE) and creates high individual financial fraud risk requiring Article 34 member notification.
Recovery Notes	Post-containment, monitor outbound connections from member management and visit-recording systems continuously for a minimum of 30 days against a documented clean baseline, with particular attention to any resumed connections to external IPs identified during the breach window. Validate that IBAN and bank account fields in restored database instances are intact and have not been tampered with or partially deleted, as attackers may have modified records to obscure exfiltration scope. Given that approximately 1 million members across six countries have had IBAN-level financial data exposed, coordinate with affected members' banks through the DPO to flag potentially compromised IBANs for transaction monitoring, and track downstream fraud reports as a recovery success metric over a 90-day window.

Forensic Artifacts	Member management application database general query log (MySQL: /var/lib/mysql/general.log or PostgreSQL: pg_log/) — filter for bulk SELECT queries against member, payment, or IBAN tables returning >500 rows, specifically identifying the authenticated database user and source host that executed them during the breach window | Web server access logs (Apache /var/log/apache2/access.log or Nginx /var/log/nginx/access.log) — filter for HTTP 200 responses to API endpoints such as '/members/export', '/members/list', or '/reports/download' with response sizes exceeding 1MB, which indicate successful bulk member record extraction via the member management web interface | Application session and authentication audit table within the member management platform's own database ('SELECT * FROM audit_log WHERE action IN ("export","bulk_read","login") AND created_at BETWEEN breach_start AND breach_end ORDER BY created_at;') — this captures the application-layer identity of whoever performed the data access, which may differ from the OS-level or database-level user | Network perimeter firewall or proxy logs showing sustained outbound TCP sessions (duration >5 minutes, bytes_out >10MB) originating from the member management system's IP address to non-RFC1918 destinations during off-hours, consistent with T1041 (Exfiltration Over C2 Channel) or T1567 (Exfiltration Over Web Service) behavior | Visit-recording system event logs — since Basic-Fit's visit-recording system was explicitly named as compromised alongside the member management system, capture any data sync, API call, or scheduled export logs from the visit-recording platform that could indicate it served as a pivot point or secondary exfiltration source for member PII

Per-Action IR Details

Containment — If your organization operates member management, fitness, or subscription-based CRM platforms with stored bank account or payment data, audit current access controls immediately. Identify and revoke any anomalous or unauthorized account sessions. Isolate affected systems from production if forensic investigation is ongoing.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST AC-17 (Remote Access), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Run 'Get-WinEvent -LogName Security -FilterXPath '*[System[EventID=4624 or EventID=4625 or EventID=4648]]'" on the member management system host to enumerate active and recent sessions. Export active sessions on Linux-based CRM backends with 'who -a' and 'last -a | head -50'. Use osquery 'SELECT * FROM logged_in_users;' and 'SELECT * FROM user_ssh_keys;' to identify persistent session tokens or SSH keys that should not exist. Block inbound connections to the member management system at the host firewall using 'ufw deny from ' or Windows Defender Firewall 'netsh advfirewall firewall add rule'.

Evidence: Before revoking sessions, capture a full snapshot of active authenticated sessions in the member management platform's application session table (database query: 'SELECT session_id, user_id, ip_address, created_at, last_activity FROM sessions ORDER BY last_activity DESC;'). Preserve the web server access logs (Apache: /var/log/apache2/access.log; Nginx: /var/log/nginx/access.log; IIS: C:\inetpub\logs\LogFiles\) showing the IP addresses and user-agents that performed bulk member record reads or export requests. Capture a memory image of the application server if the breach is suspected to be recent and active, to identify in-memory credential tokens or live attacker sessions.

Detection — Review authentication logs on member management and data repository systems for anomalous access patterns: bulk data reads, unusual export volumes, off-hours access, or access from unexpected IP ranges. Correlate against T1078 (Valid Accounts) indicators — look for credential use outside normal geographic or time baselines. Query SIEM for large outbound data transfers (T1041, T1567) from systems housing member PII or financial data.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, query the member management database directly for anomalous read volumes: 'SELECT user, COUNT(*) as query_count, SUM(rows_examined) as rows_examined FROM mysql.general_log WHERE command_type="Query" AND argument LIKE "%member%" GROUP BY user ORDER BY rows_examined DESC;'. Use GoAccess (free, CLI-based) to analyze web server access logs for bulk export URIs: 'goaccess /var/log/nginx/access.log --log-format=COMBINED -o report.html'. For outbound transfer detection without EDR, capture a 60-minute tcpdump on the member management server's NIC: 'tcpdump -i eth0 -w /tmp/capture_$(date +%F).pcap "not port 443 and dst net not 10.0.0.0/8"' and analyze with Wireshark filtering on large payload sizes. Apply the public Sigma rule 'win_security_susp_failed_logon_reasons.yml' against Windows Security Event Log exports if the CRM runs on Windows.

Evidence: Preserve application-level API gateway or load balancer logs showing the specific endpoints queried (e.g., '/api/members/export', '/api/members/search?limit=10000'), including timestamps, source IPs, authenticated user tokens, and HTTP response sizes — large response bodies (>1MB) on member list endpoints are a primary indicator. Extract database slow query logs and general query logs from the MySQL/PostgreSQL instance backing the member management system, filtering for SELECT statements against tables containing 'bank_account', 'iban', or 'payment' columns. Capture NetFlow or connection state logs from the network perimeter showing sustained outbound TCP connections from the member management system's IP to non-EU external IP ranges, which would indicate T1041 exfiltration channels.

Eradication — Reset credentials for all accounts with access to member management and visit-recording systems. Enforce MFA on all administrative and data-access accounts. Review and tighten data access permissions to least privilege. Confirm no persistent attacker footholds remain via endpoint and network forensics.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST IA-5 (Authenticator Management), NIST AC-6 (Least Privilege), NIST SI-2 (Flaw Remediation), CIS 5.2 (Use Unique Passwords), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Enumerate all database accounts with SELECT privileges on member PII tables: 'SELECT grantee, table_schema, table_name, privilege_type FROM information_schema.table_privileges WHERE table_name IN ("members","bank_accounts","visit_records") ORDER BY grantee;' — revoke any not operationally required. Use TOTP-based MFA (e.g., Google Authenticator paired with PAM module 'libpam-google-authenticator') for SSH access to member management servers at zero cost. Deploy a YARA rule scanning the web root and application directories for webshells: 'yara -r webshells.yar /var/www/html/' using the Neo23x0 public YARA ruleset. Check for persistence via cron: 'crontab -l -u www-data' and 'ls -la /etc/cron.*/' on all application servers. On Windows CRM hosts, run 'Get-ScheduledTask | Where-Object {$_.TaskPath -notlike "\Microsoft*"}' to identify non-standard scheduled tasks.

Evidence: Before credential reset, capture the full list of accounts that had authenticated access to the member management system and visit-recording system during the breach window, including service accounts and API keys, from the application's own user management database table. Preserve SSH authorized_keys files ('cat /home/*/.ssh/authorized_keys; cat /root/.ssh/authorized_keys') and web server configuration files to detect backdoored accounts or injected SSH keys added during the attacker's access window. Collect a directory listing with timestamps ('find /var/www -name "*.php" -newer /var/www/html/index.php -ls') to identify any webshells or malicious scripts uploaded to the member management application during the intrusion period.

Recovery — Validate that data exfiltration has ceased by monitoring outbound traffic baselines. Confirm integrity of member data stores. Notify affected members per GDPR Article 34 obligations where breach poses high risk to individuals. Coordinate with legal and DPO to meet GDPR Article 33 supervisory authority notification deadline (72 hours from confirmed discovery) in each affected jurisdiction.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IR-6 (Incident Reporting), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-11 (Audit Record Retention), CIS 3.4 (Enforce Data Retention)

Compensating: Establish a outbound traffic baseline for the member management system by capturing 'ss -tunp' output every 5 minutes via cron for 48 hours post-remediation and alerting on any new external destination IPs not present before the breach. Verify database integrity by running row counts and checksum comparisons on member tables against the most recent pre-breach backup: 'SELECT COUNT(*), SUM(CRC32(CONCAT(id, email, iban))) AS checksum FROM members;' — compare against equivalent query on backup. For GDPR Article 33 coordination across six jurisdictions (NL: Autoriteit Persoonsgegevens; BE: APD; LU: CNPD; FR: CNIL; ES: AEPD; DE: respective Landesbeauftragter), document breach discovery timestamp precisely and initiate DPA notifications within 72 hours using each authority's online breach notification portal.

Evidence: Preserve complete, timestamped outbound connection logs from the recovery window to demonstrate to GDPR supervisory authorities that exfiltration ceased at a documented point in time — this is a regulatory evidentiary requirement under GDPR Article 33(3)(b) for describing measures taken to address the breach. Generate a before/after record count and field-level integrity report from the member management database to quantify exactly which records and which data fields (name, address, email, phone, DOB, IBAN) were accessible during the breach window, which is required for GDPR notification content specifying 'the categories and approximate number of data records concerned.' Retain all network flow logs and authentication logs from the breach window for a minimum of 12 months to support potential regulatory investigations by the six national DPAs.

Post-Incident — Conduct a data minimization review: assess whether bank account data retention in member management systems is operationally necessary and aligned with GDPR data minimization principles (Article 5(1)(c)). Implement data-at-rest encryption for PII and financial data fields. Establish a continuous monitoring control for bulk data access anomalies. Review third-party data processor agreements for all vendors with access to member data.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-12 (Information Management and Retention), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SC-28 (Protection of Information at Rest), CIS 3.2 (Establish and Maintain a Data Inventory), CIS 3.6 (Encrypt Data on End-User Devices), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Implement field-level encryption for IBAN and bank account columns in the member management database at zero cost using MySQL's built-in AES_ENCRYPT/AES_DECRYPT functions or PostgreSQL's pgcrypto extension ('CREATE EXTENSION pgcrypto; UPDATE members SET iban = pgp_sym_encrypt(iban, "key");'). For continuous bulk-access monitoring without SIEM, deploy a MySQL audit plugin (MariaDB Audit Plugin, free) configured to log all SELECT statements returning more than 100 rows from member tables, writing to a separate audit log file reviewed daily. Schedule a weekly automated data inventory script using osquery ('SELECT * FROM file WHERE path LIKE "/var/backups/%" AND size > 10000000;') to detect unexpected large data files that may indicate unauthorized exports. For third-party processor review, cross-reference your GDPR Article 28 processor agreements against the current list of API keys and database credentials active in the member management system.

Evidence: Produce a data flow map documenting every system, service account, and third-party integration that had read access to the IBAN/bank account fields and visit-record tables during the 12 months preceding the breach — this artifact is required for the lessons-learned report and supports regulatory accountability obligations under GDPR Article 5(2). Retain the forensic images, log archives, and network captures from this incident for a minimum of three years given the multi-jurisdictional GDPR regulatory exposure across six EU member states, as investigations by national DPAs may be initiated months after the initial notification.

Detection Guidance

No confirmed IOCs have been publicly released for this breach. Detection should focus on behavioral and anomaly-based indicators rather than known-bad signatures. Key queries: (1) SIEM, alert on bulk SELECT or export operations against member database tables exceeding baseline row thresholds; (2) Identity logs, flag authentication events for service accounts or admin accounts outside established working hours or originating from new geographic locations (T1078); (3) DLP/proxy, monitor for large outbound data transfers to external destinations from systems hosting member PII, particularly via HTTP/HTTPS (T1041, T1567); (4) Cloud storage logs, if member data resides in cloud repositories (S3, Azure Blob, GCP Storage), enable and review access logs for unusual read volumes or access from new principals (T1530); (5) Email logs, review for bulk export or forwarding rules applied to accounts with access to member data (T1114). Confidence in detection is limited by the absence of confirmed attack vector and published IOCs.

Framework Mappings

MITRE-ATTACK

- **T1005** — Data from Local System
- **T1114** — Email Collection
- **T1078** — Valid Accounts
- **T1567** — Exfiltration Over Web Service
- **T1530** — Data from Cloud Storage
- **T1213** — Data from Information Repositories
- **T1041** — Exfiltration Over C2 Channel

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(6)(ii)** — Response and Reporting

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process

- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC7.4** — Responds to identified security incidents

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated
- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1005	Data from Local System	Collection
T1114	Email Collection	Collection
T1078	Valid Accounts	Defense-Evasion
T1567	Exfiltration Over Web Service	Exfiltration
T1530	Data from Cloud Storage	Collection
T1213	Data from Information Repositories	Collection
T1041	Exfiltration Over C2 Channel	Exfiltration

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/european-gym-giant-b...	T3
Hack at Dutch gym chain Basic-Fit exposes customer data ...	https://therecord.media/dutch-gym-chain-basic-fit-hit-by-hackers	T3
Basic-Fit data breach exposes details of a million gym ...	https://ca.finance.yahoo.com/news/basic-fit-data-breach-exposes-091...	T3

Source	URL	Tier
Gym operator Basic-Fit data breach exposes details of a ...	https://m.economictimes.com/tech/technology/gym-operator-basic-fit-...	T3
Basic-Fit data breach exposes details of a million gym ...	https://www.channelnewsasia.com/business/basic-fit-data-breach-expo...	T3

Generated 2026-04-14 06:04 UTC by TJS Security Command Center