

The **Revolut** Incident

How exposed KYC data can become fraud infrastructure for the entire financial sector.

REPORT VERSION 1.0 / INFORMATION CURRENT AS OF 17 SEPTEMBER 2026

This report reflects publicly available information at the time of publication and may be updated as new details emerge.

EXECUTIVE SUMMARY

This is now an industry-wide fraud risk

What happened: Fraudulent requests from a legitimate government-agency email domain caused sensitive Revolut customer data to be disclosed.

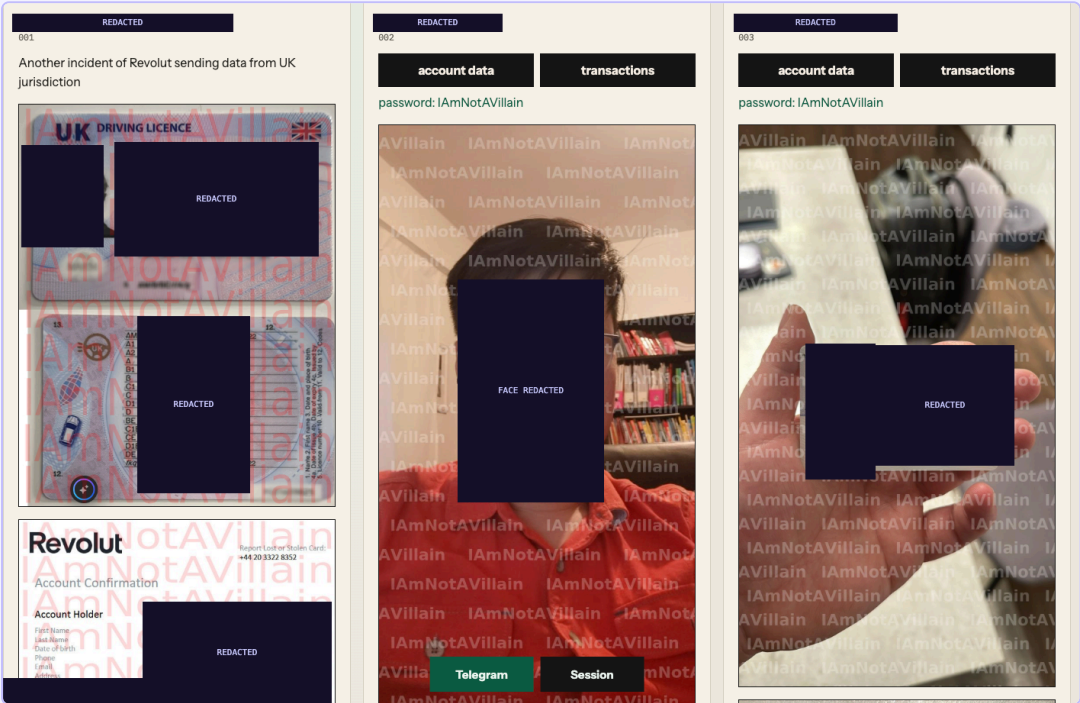
What has changed: A genuine document may establish that an identity exists. It does not prove that the person presenting it controls that identity.

Why it matters to you: The exposed identity materials may be reused to impersonate customers and open or recover accounts at other financial institutions.

What to do now: Strengthen disclosure workflows, monitor for identity reuse and use additional intelligence before relying on document-heavy verification.

REPORTED LEAK MATERIAL / FULLY REDACTED

ACCESSED 16 SEP 2026



A public site claiming to release Revolut customer records displayed identity documents, selfies and account information. Heka has not independently verified the material. All identifying information has been removed.

CONFIRMED BY REVOLUT

Fraudulent requests came through a legitimate agency email domain; systems and customer funds were unaffected.

REPORTED BY THE MEDIA

Exposed material reportedly included identity documents, contact details, selfies, statements and financial information.

CLAIMED BY THE ACTORS – UNVERIFIED

The actors claimed a larger dataset, prolonged access and further releases.

This was a decision-layer attack

The attacker did not need to defeat Revolut's perimeter if a trusted-looking request could cause an authorised process to release customer data.

ATTACK PATH

TRUSTED REQUEST → EXTERNAL LEVERAGE

1

Trusted channel

Request appears to come from an authentic agency domain.

2

Plausible authority

The sender appears entitled to request information.

3

Internal release

A valid process retrieves and transmits customer data.

4

External leverage

The data can enable targeting, impersonation or extortion.

THREAT-ACTOR SITE / RECREATED + REDACTED

UNVERIFIED CLAIMS

"We have everything..."

Claimed categories included KYC documents, addresses, contact details, bank accounts and transaction histories.

KYC documents

Addresses

Contact details

Bank accounts

Transaction histories

No leaked personal data is reproduced or linked in this report.

Customers are not waiting for the investigation

Most of the criticism is about the incident itself. How the request got through, why a bank released customer files on the strength of an email, whether Revolut can be trusted at all. That anger is broad and it is not going away.

Some customers are not waiting for the investigation. They are withdrawing funds and closing accounts, and saying why.

PUBLIC DISCUSSION / R/REVOLUT

ACCESSED 16 SEP 2026

r/Revolut • 3d ago
...

Closing account after data breach

Security

I'm withdrawing all the money I had with Revolut (about 20k €) and closing my account.

It's insane that just because they received an email that said to be from a government they handed all personal information about their clients.

That's unacceptable from any company but moreover from a bank.

This happened once and it may happen again, I no longer would trust Revolut with my money and maybe you shouldn't do too.

Account closure framed as a trust decision, not a loss event.

Revolut's response led with what had not happened. Systems were untouched and customer funds were safe. That framing drew its own reaction. The money was never the exposure.

PUBLIC POST / X

ACCESSED 15 SEP 2026

Sep 13

your funds remain secured but your identity and personal details no...this is a joke lol

60

The reassurance and the grievance are about different assets.

People are asking why the files existed at all

Underneath the anger a second argument has formed, and it is the one that matters to institutions that were not breached. The discussion turned to what verification actually collects. Seeing the list in one place led customers to ask why a bank needed all of it, and how long it is kept.

WHAT STANDARD ONBOARDING COLLECTS AND RETAINS		SENSITIVITY IF DISCLOSED	
Passport	HIGH	Driving licence	HIGH
Selfie	HIGH	Address	MEDIUM
Occupation	MEDIUM	Statements	HIGH
Full transaction history			HIGH
Sensitivity is Heka's characterisation of disclosure impact, not a regulatory classification.			

THE EXPOSURE IS THE DEFAULT

The onboarding flow that produced the Revolut dataset is the standard one. Many institutions collect similar documents, for similar reasons, and hold them for similar periods. The exposure is not specific to Revolut. It is the default.

The safest sensitive data is data you never needed to collect

Document and biometric step-up can be necessary. But using it as the default response to uncertainty creates friction and accumulates high-value data. Use lower-intrusion signals first, escalating only when risk remains unresolved.

TIER	ESCALATION PATH	DATA + FRICTION COST
01	EXISTING CONTROLS Device, behavioural, bureau and internal-account signals	 LOWEST
02	EXTERNAL IDENTITY INTELLIGENCE Net-new web and digital-footprint signals; no new customer document	 LOW
03	TARGETED STEP-UP Request a selfie or identity document only where uncertainty remains	 HIGH
04	MANUAL INVESTIGATION Reserve the highest-cost path for the smallest queue	 HIGHEST

DESIGN PRINCIPLE

Use more intelligence before collecting more identity data.

Resolve identity uncertainty without another upload

Heka adds net-new identity intelligence from publicly available web sources and relevant digital signals. It complements existing KYC, device and bureau controls; the financial institution retains the decision.

HEKA CASE VIEW / ILLUSTRATIVE SAMPLE

CASE HK-4471 • 2026-09-02 14:12 UTC

IDENTITY RISK SCORE

74 / 100

0 PASS REVIEW 100 HIGH RISK

DECISION • REVIEW

Sample values for illustration.
Signal weights sum to the score.

Email address first seen 6 days ago

+18

Digital footprint • 2026-09-02 14:11 UTC

No social presence linked to the claimed name

+16

Social • 2026-09-02 14:11 UTC

Phone number appears in three breach records

+14

Darknet breach • 2026-09-02 14:12 UTC

Claimed employer has no verifiable web presence

+11

Contact • 2026-09-02 14:12 UTC

A LOWER-DATA STEP-UP PATH

Ambiguous case

>

Heka intelligence

>

Risk evidence

>

Decision

No additional customer selfie or identity document is required for Heka's analysis.

Net-new identity signals

Extend beyond static internal and bureau records.

Attributable evidence

Surface reason codes and supporting context.

Global by design

Assess complex and mobile identities.

Stack-compatible

Add intelligence without replacing decision logic.

ASSESS YOUR EXPOSURE

Identify where document-heavy step-up can be replaced or deferred with net-new identity intelligence.

What financial institutions can do now

READ
THIS
FIRST

This is no longer only Revolut's problem. Exposed Revolut customer data may be used to commit identity fraud at other banks, lenders and card issuers.

HORIZON	ACTION
48 HOURS	Contain and scope Inventory exceptional disclosures; validate requesting authorities through a second channel; identify subjects and downstream exposure.
30 DAYS	Harden the workflow and prepare for cross-institution reuse Assume that identity data exposed by another institution may be presented to yours. Require independent verification and dual approval for sensitive disclosures, strengthen checks for customers presenting previously exposed identity attributes, and monitor for unusual reuse across onboarding, account recovery and high-risk transactions.
90 DAYS	Reduce stored sensitivity Map document, selfie and statement collection; challenge default retention; add a lower-data intelligence tier before document step-up.
ONGOING	Test the decision layer Red-team legal and government-request workflows; measure exceptions; rehearse notification and high-risk victim support.

NEXT STEP

See where a lower-data intelligence tier fits your decision layer.

We reply within one business day.

CONTACT

info@hekaglobal.com

SOURCES

Reuters, 12 Sep 2026
(updated 14 Sep)

Financial Times, 15
Sep 2026

Public discussion on
r/Revolut, accessed 16
Sep 2026

YC Hacker News Forum,
accessed 16 Sep 2026

TechCrunch, 12 Sep 2026

Cybernews, 15 Sep 2026

@internationalcyberdigest,
X, accessed 15 Sep 2026

AHEKA

Heka finds sophisticated third-party identity fraud that existing controls miss, and returns one explainable identity risk score with every signal shown.

Threat-actor allegations are unverified. This report is informational and is not legal or cybersecurity advice.