TLP:CLEAR

RED HOT CYBER · DARK LAB

The Revolut and Kraken cases

27 wallets, 27 attack surfaces

Cyber Threat Intelligence Report
Case analysis and operational recommendations

September 2026 · v1.0

Olivia Terragni · Edoardo Faccioli · Luca Stivali · Raffaela Crisci

Introduction

«27 wallets d'identité = 27 surfaces d'attaque.
La fuite Revolut me le confirme :
la souveraineté se joue dans l'exploitation.»
— Dear Vincent (@StarryCook), X, 16/09/2026.

This dossier reconstructs two concrete cases — the Revolut incident (2026) and the earlier Kraken case (2025) — with the aim of turning the analysis of the attack into an operational tool for defence.

In both scenarios, customers' sensitive data became a lever of attack without any direct breach of IT systems. In the Revolut case, the compromise occurred through falsified requests sent from an institutional PEC (certified email) mailbox; in the Kraken case (2026), through the abuse of internal access to support systems. At the heart of this report lies a regulatory paradox: the information that KYC/AML obligations (anti-money-laundering directives) require to be collected in order to protect the system (identities, documents, transactions) is the very same information that, once handed to the wrong party, exposes the user. Hence the document's dual nature: a factual analysis of the events and a reference framework for financial operators.

The primary attack vector is the abuse of the trust channel. Malicious requests exploit the implicit trust placed in an official sender (PEC, government-body email, or telephone spoofing). Between the receipt of the request and the release of the data, a critical process gap opens. Verifying a request coming from the authorities is complex, caught between the regulatory duty of rapid cooperation and the lack of tools for reliable authentication. To this is added human error: in at least one documented step, the data was transmitted by replying directly to the compromised address, without activating independent verification channels (e.g. out-of-band). These are procedural failures.

In a chain of trust between public authorities and financial institutions, which controls fell to each link — the entity that owns the channel, the bank that discloses the data, the regulatory framework governing the requests — and which ones failed? Although the technical compromise concerns the sender, the rules (starting with the GDPR) place on the financial institution, as data controller, a qualified responsibility over customers' data — without excluding that of the other links in the chain.

This obliges banks to implement independent procedural checks — precisely what was missing in the step cited. The limit of traditional controls in the face of attacks based on stolen institutional credentials (e.g. via infostealer) is forcing a paradigm shift in the sector. An emblematic case is the integration of Dark Web Intelligence into Anti-Financial Crime processes: the recent strategic partnership between Nasdaq Verafin and Q6 Cyber highlights the systemic need to monitor the criminal underground to intercept data leaks pre-emptively, filling that procedural “grey zone” exploited in the cases analysed here.

The last link in the chain is reputational impact. The stolen data is used not only as merchandise in the underground market, but as an extortion lever: public ransom demands and media pressure on institutions exposed on the capital markets (valuations, listings, investor confidence). Since the technical executor of the attack, the extortionist and the media amplifier do not necessarily coincide, the report keeps these levels separate, leaving the attribution of motive open.

The methodological perimeter rests exclusively on open sources (OSINT/CTI). Every statement is accompanied by a level of analytical confidence (High, Medium, Low), separating proven facts from the claims of threat actors, which are treated as interested-party sources and not as evidence. No personal data of the victims is reproduced.

Finally, the analysis raises a fundamental strategic question: cui prodest? Is the real target of these campaigns the financial institution's database — for the mere monetisation of the data — or the chain of trust itself between public authorities and private entities? The distinction is not secondary: if the objective

were the channel, and not the individual record, the damage should be read on a systemic plane — structural doubt, slower cooperation between law enforcement and banks, the compliance obligation turning into a surface of vulnerability — a dynamic that would exceed simple extortion. It is a hypothesis to be kept open, not a conclusion: the available findings do not allow us to establish whether this is opportunistic monetisation or a deliberate targeting of the trust channel. The document has no accusatory purpose, nor does it establish legal liability; where facts are not ascertained, it states so explicitly. As this is a dynamic threat landscape, the present work is to be regarded as continuously evolving.

Olivia Terragni

Contents

1. 1. Executive summary

> The Revolut case is not merely a “data breach” in the classic sense: it is a case of social engineering through the abuse of an institutional channel and a possible failure of the controls verifying requests. Revolut stated that customers' funds and its own systems were not compromised, but that sensitive data was handed to an unauthorised party following fraudulent requests apparently coming from a legitimate government domain (Reuters, 12/09/2026). The scheme is not isolated and finds a strong parallel in the earlier Kraken incident (2025). On that occasion, the exfiltration of data did not go through a breach of the primary security perimeter, but through the abuse of internal access to support systems. Both scenarios confirm a precise trend: attackers bypass core technological defences to strike directly at trust-based processes and assistance procedures.

Confidence scale

Level	Meaning
High	Multiple concurring independent sources, or a primary source (company statement, judicial act, verifiable technical data)
Medium	A credible but single source, or multiple sources deriving from the same material (screenshots, third-party statements) without official confirmation
Low	Claim by the attacker or by interested intermediaries, unverified; or an inference with contrary elements

- **[High confidence]** The attack exploited the process of responding to requests from the authorities, not a compromise of Revolut's core systems or funds. — Basis: Revolut statement; Reuters; published PEC messages
- **[Medium confidence]** The requests ‘reportedly’ originated from an Italian institutional PEC mailbox (attributable to the Local Authorities Office of the Prefecture of Reggio Calabria) and reportedly included fake European Investigation Orders in the name of the Milan Public Prosecutor's Office, in the period March–July 2026. The attacker also claims to have obtained data on 680 customers, probably selected after analysis of the blockchain and transactions; this figure and the selection method have not been officially confirmed by Revolut. — Basis: PEC screenshots; StrettoWeb; Silere non possum; attacker statements
- **[High confidence]** The scheme is not isolated: in 2025 Kraken reportedly handed over data on a customer after receiving fake requests from an @interno.it address, followed by physical threats. — Basis: filing CGC-26-634771, San Francisco Superior Court. The high confidence concerns the existence and content of the episode documented in the filing; it does not imply that the Kraken episode and the Revolut one were carried out by the same group.
- **[Medium confidence]** The actors show indicators of limited operational discipline — neglected infrastructure, public conflict between groups, and a template-based website — but the success of the operation depends above all on the institutional channel exploited and does not necessarily demonstrate an overall low technical capability. — Basis: KELA; Duel; site code; WHOIS
- **[Medium confidence]** The risk is replicable towards other institutions that receive requests from the authorities via PEC or email, including Italian banks. The circulation of institutional credentials in infostealer logs and combolists is indicated by threat-intelligence sources and prior advisories, but the direct link with the PEC in the Revolut case is not publicly demonstrated. — Basis: CERT-AGID; sector TI source; FBI 2024

2. Timeline of the incident

Date	Event	Confidence
May–July 2025	Kraken receives a fake request from "@interno.it"; hands over data; physical threats to the customer; in August, a fake Irish order	High (judicial act, actor's version)
06/03/2026	Doe v. Kraken lawsuit filed: the scheme becomes public (press release 16/03)	High
24/03/2026	PEC exchange between Revolut and @pec.interno.it: Revolut indicates the request should be re-addressed to the Cypriot crypto company	Medium (screenshot)
04–05/05/2026	Fake European Investigation Order “Milan Public Prosecutor's Office” to Revolut Bank UAB; about 40 messages	Medium
24/07/2026	Revolut sends encrypted data to entilocali.prefrc@pec.interno.it; distinction by jurisdiction (169 hashes Revolut Ltd, 29 Swiss entity)	Medium (screenshot)
12/09/2026	Revolut confirms the delivery of the data and blocks the address	High
13/09/2026	First publications on Telegram (“Example 1”); creation of the “smile” channel	High
14/09/2026	Extortion site; imnotavillain[.]xyz registered; Revolut Smilik contacts City AM; Telegram removal request from 8 companies; ICO report received: "We can confirm we have received a report and are assessing the information provided." Euronews (16/09)	High
15/09/2026	iamnotavillain[.]com registered; the Italian press identifies the Prefecture's PEC; the Postal Police investigates	High
16/09/2026	Ransom of 6,000 XMR / 3 million dollars with a countdown; video of the material; shutdown of GitHub, Telegram channels and the group's site; new domain with data on 12 customers. In parallel, the third-party information site iamnotavillain[.]info appears, with its own countdown towards 21/09.	Medium
17/09/2026	The group's extortion-site 24-hour deadline expired at 18:30; the site goes offline. Revolut states it received no direct contact or requests from the group (FT/CoinDesk; Reuters).	Medium
18/09/2026	Investigative sources reported by the press: the Postal Police found no flaws in the Ministry of the Interior's systems and initial findings do not confirm the exfiltration of the 147 GB; it remains to be established whether the mailbox was compromised or cloned. The data-protection	Medium

Date	Event	Confidence
	Authority (Garante) opens checks on Italian banks' access practices, sends a communication to bank DPOs, opens an exchange with the Lithuanian authority and a dialogue with the Ministry of the Interior.	
19/09/2026	Parliamentary answer: the Under-Secretary for the Interior Wanda Ferro reports (Pastorella question, Azione) that the Ministry's cyber-security structures are carrying out initial in-depth checks, under confidentiality, and that the ACN is in contact with Revolut and cooperating with the Ministry, having informed the Postal Police and the DNAA. The information site iamnotavillain[.]info shows a countdown still active (≈40 h) towards 21/09.	Medium
23/09/2026	Put up for sale: on the Exploit.IN forum an ad under the name «fullcowgirl» appears, offering the database of ~700 Revolut customers (KYC + PII) for 300,000 USD in XMR/BTC, with a sample watermarked «IAmNotAVillain». The ad states uses for home invasion, phishing, identity theft and extortion. Flagged by S2W DailyThreat (S2W Inc., CTI, South Korea). Content and list of subjects: seller's claim, unverified.	Medium-high

According to public reconstructions, the Revolut case may fit into a broader scheme of abuse of institutional mailboxes and of the processes by which banks, exchanges and fintechs respond to requests from the authorities. Some reconstructions link earlier requests directed at crypto platforms to the use of addresses belonging to institutional domains; these links must however be verified case by case and cannot automatically be presented as part of a single campaign.

In 2025, according to the available reconstruction, Kraken reportedly received a request from an address on the interno.it domain and reportedly transmitted data on a customer, who subsequently reportedly received physical threats. In 2026, the scheme reportedly continued through an institutional PEC on the pec.interno.it domain and documents presented as European Investigation Orders. In the Revolut case, journalistic reconstructions indicate that fraudulent requests were reportedly used to obtain, over a prolonged period, KYC files of high-net-worth customers selected through public blockchain information. These elements suggest possible operational continuity, but the link between the various episodes remains a hypothesis to be verified. In September the case exploded: the actors (IAmNotAVillain, Revolut Smilik) move to extortion and publication of the data, a crypto casino (Duel) obtains privileged contact with the hacker, and vendors, media and third-party accounts amplify the incident. The claims about the number of victims, the selection of customers via blockchain and the possible compromise of other systems must be classified separately as attacker statements, journalistic reporting, or elements not yet confirmed.

The end point is political-normative: Lyudmyla Kozlovska, Ukrainian human-rights activist and founder and president of the Open Dialogue Foundation (ODF), uses the case as evidence that the verification of state requests is impossible and that FATF, anti-money-laundering and DAC8 rules must be changed. This passage should be presented as a reading or a position in the public debate, not as proof that the rules are causally responsible for the incident. Lyudmyla Kozlovska provides a political-normative reading of the case. Her statements are relevant to the debate on the verification of state requests, judicial cooperation and transnational financial repression.

The central analytical point is the possible abuse of the chain of trust between public authorities and financial operators. If a request is considered authentic merely because it comes from an institutional domain or mailbox, the technical verification of the sender can become insufficient. The connections between the various episodes remain analytical hypotheses; the individual elements are documented in the following sections.

Updated to 20 September 2026. Material collected from open sources, judicial documents, DNS and network data, social posts, screenshots and messages received.

The critical point (hypothesis)

PEC certifies the sending, delivery, integrity of the message and the traceability of the transmission to the sender's PEC address, but it does not automatically identify the person who drafted the content, nor does it guarantee that they were authorised to do so. Identifying the author of the document requires a further element, normally a qualified digital signature or another verifiable mechanism. In the Revolut case, the available screenshot of an alleged information-production order (EIO) shows no digital signature or clearly identifiable stamp and is written in English; on the basis of public information, it is not known whether the requests actually received by Revolut contained digitally signed attachments. The direct transmission to Revolut's Italian PEC, rather than to the competent executing authority of the indicated State (Lithuania), appears incompatible with the normal mechanism for the recognition and execution of the EIO (Dir. 2014/41/EU, Art. 9) and should have required additional checks. On its own, however, it does not prove that the document was false: one must verify the sender, the signature, the standard form (Annex A), the issuing authority and any official contacts between the authorities.

A further indicator of internal inconsistency: in the image of the EIO that circulated — not independently verified as the one actually received by Revolut — the issuing authority indicated is the «Public Prosecutor's Office at the Court of Milan», while the sender mailbox is attributable to the Ministry of the Interior and, in particular, to the locality of Reggio Calabria, over 1,200 km from Milan. The gap between the authority named in the document and the office from which the transmission originated is an element of suspicion about the genuineness of the act, to be assessed together with the signature, the standard form (Annex A) and the issuing authority. [Medium confidence — Basis: Jason Mikula / Fintech Business Weekly, 20/09/2026]

REPUBBLICA ITALIANA

EUROPEAN INVESTIGATION ORDER (EIO)

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014
regarding the European Investigation Order in criminal matters

Issuing Authority: Public Prosecutor's Office at the Court of Milan
(competent pursuant to Legislative Decree 108/2017)
Address: Via Freguglia 1, 20122 Milano, Italy
Reference / Protocol: Prot. n. [redacted]/2026
Date: 4 May 2026

Issuing State: Italian Republic
Executing State: Republic of Lithuania
Recipient Executing Authority: General Prosecutor's Office of Lithuania or the competent Lithuanian authority for financial investigations / Revolut Bank UAB
Revolut Bank UAB registered address: Konstitucijos pr. 21B, Vilnius, LT-08130, Lithuania

Subject

Request for the acquisition of banking and financial information relating to the following deposit addresses associated with accounts held with Revolut Bank UAB (an entity registered in Lithuania).

Deposit Addresses (wallets):	[redacted]

PEC: what it certifies and what it does not

Unlike ordinary email, the sender field of a PEC message cannot be falsified from outside (spoofing). A message is valid only if it actually originates from a real PEC mailbox and is processed by its accredited provider, which signs it digitally and generates the acceptance and delivery receipts. It is therefore not technically possible to forge the sender entilocali.prefrc@pec.interno.it without having direct access to that specific mailbox or to the infrastructure that hosts it.

PEC, by its nature, certifies the sending, the delivery, the integrity of the content and the validity of the sender mailbox. However, it does not certify the physical identity of the person typing the text, nor their legitimacy to formulate the request.

This is the fundamental distinction between the authenticity of the channel (technically flawless) and the legitimacy of the sender (in this case, fraudulent). It follows that, if the messages received by Revolut were authentic PEC, the government mailbox was genuinely under the control of the threat actors (Account Takeover hypothesis); how they gained access to it remains under investigation.

Finally, it should be noted that the technical verification of this compromise can only be carried out by analysing the full headers and the transport envelope signed by the provider: elements not currently present in the material available from open sources. **[High confidence]** — Regulatory basis: Presidential Decree 68/2005 and Technical Rules (Ministerial Decree 2/11/2005).

Note — authenticity of the sender address. On the group's site the mailbox address is redacted; the full address (entilocali.prefrc@pec.interno.it) circulated via a screenshot attributed to Korra/Duel and the Italian press — it was not “guessed”. Since those images are curated and watermarked by the actors, the address cannot be considered authentic on the basis of the screenshots alone: in principle the mailbox shown might not coincide with the one actually used.

Three elements independent of the images, however, argue for its reality: a valid PEC message originates only from a genuinely existing mailbox (an invented address would not generate valid PEC messages); the address follows the actual convention of the Prefectures (entilocali.pref<code>, cf. Cosenza) on interno.it, managed by InfoCert; investigators treat the mailbox as real, assessing how it was accessed, not whether it exists.

Operational conclusion:the address is to be considered real and existing on the grounds of PEC validity, convention and third-party corroboration, not on the basis of the group's images. Certainty that the mailbox shown is exactly the one used can come only from the transport envelope/logs of the PEC provider. [Medium-high confidence on the mailbox's existence; low on the exact identity derivable from the screenshots] — Basis: screenshot attributed to Korra/Duel; press; PEC convention of the Prefectures; PEC rules

Kraken / Revolut comparison

Kraken and Revolut show two successive and potentially related applications of the abuse of apparently institutional requests against crypto operators. The Revolut case presents a more evolved channel — PEC, a formal judicial document and large-scale targeting — but the available material does not prove that the two episodes were carried out by the same actor.

Confirming the sensitive market phase, at the time of the contested requests (May–August 2025) Kraken's IPO trajectory was already public: a stated target for the first quarter of 2026 (March 2025) and a 500-million-dollar round at a 15-billion valuation in September 2025. On 3 February 2026 Kraken also published, while remaining private, listed-company-style reporting — adjusted 2025 revenues of 2.2 billion dollars (+33% year-on-year) and adjusted EBITDA of 531 million — before the IPO pause in March 2026.

[High confidenceon Kraken's IPO and financial data] — Basis: Bloomberg (07/03/2025); Fortune (25/09/2025); Kraken press release (03/02/2026).

Aspect	Kraken (2025)	Revolut (2026)
Type of company	Crypto exchange	Fintech with banking licences (United Kingdom, Lithuania, France) and a crypto company in Cyprus
Market phase before the attack	Preparing for the IPO: public trajectory since March 2025, stated target Q1 2026	Preparing for a possible dual listing (London + Wall Street), horizon indicated at 2028
Period and sequence of the attack	Spoofed emails May–August 2025 → extortion/surveillance (2025); confidential IPO filing announced in April 2026, then postponed towards 2027	Requests from PEC (ref. 24/03 and 24/07 2026), a data-collection campaign lasting ~5–6 months according to the actor's claim → breach and ransom demand (September 2026)
Type of incident	Delivery of data to emails that appeared to come from an Italian law-enforcement agency	Delivery of data to requests sent from an authentic PEC on an Italian institutional domain (Prefecture of Reggio Calabria)
Technical vector	Sender spoofing: counterfeit emails with law-enforcement branding, falsified sender	Abuse of a certified channel: real PEC (entilocali.prefrc@pec.interno.it); authentication appears aligned because the mail passes through the genuine channel
Mailbox of the fake authority	Ordinary address @interno.it	24/03: @pec.interno.it (redacted) with a copy to @interno.it; 24/07: entilocali[.]prefrc[@]pec.interno.it
Company mailbox	lawenforcement[@]kraken[.]com	revolut[.]italy[.]pec[@]legalmail[.]it
Document presented	“Information request”, followed by an alleged Irish order	Alleged European Investigation Orders in the name of the Milan Public Prosecutor's Office
Request method	Single customer	Hundreds of transaction IDs and deposit addresses used as search keys (“spray and pray”)
Target	Customer with a high-value account	Crypto holders (“whales”) among the customers, with high balances
Data exposed	Name, date of birth, address, phone, account information	KYC and financial data of ~680 European customers: passports, KYC selfies, IBANs, transaction history
Additional actor claims [unconfirmed]	No large-scale public claim; the affair emerges through the customer's civil lawsuit	147 GB exfiltrated from Italian law-enforcement systems and use of a RAT; campaign lasting ~6 months
Official confirmations	Public lawsuit; Kraken has not denied the basic dynamic (spoofed emails, data disclosure)	Revolut has confirmed the breach and the delivery to fraudulent requests from an authentic government domain; no official confirmation on the 147 GB
Subsequent extortion	Data used for extortion/surveillance: threats, surveillance, attempted entry into a home	Demand for 3 million dollars (indicated as ~6,000 XMR), 24h ultimatum expired on 17/09/2026; the attackers' site then offline

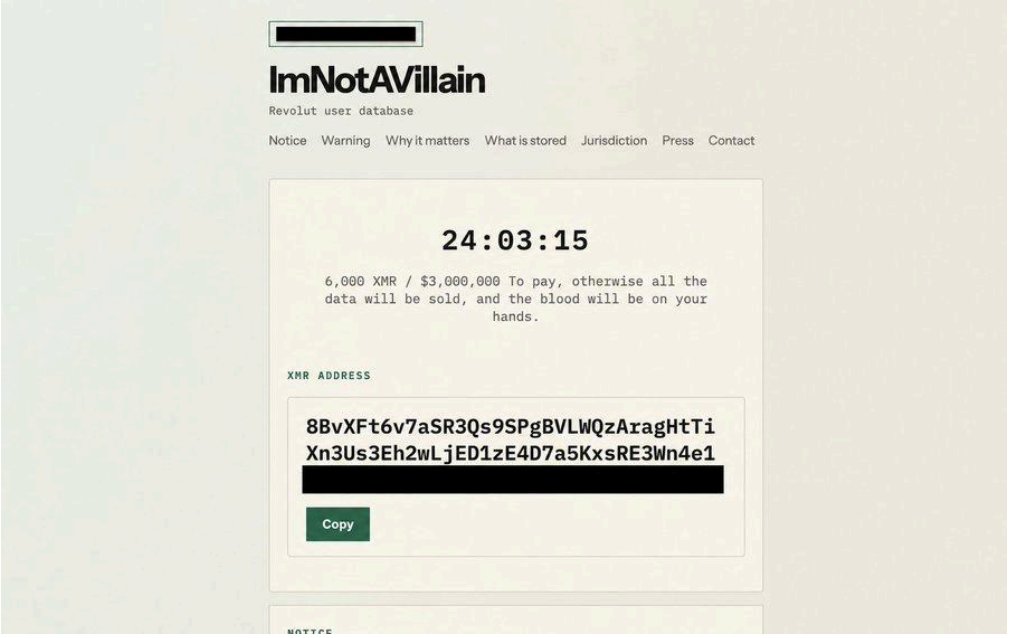
Involvement of Italian authorities	No known public Italian investigation into the spoofed email; the lawsuit is in the USA	Investigation by the Reggio Calabria Public Prosecutor's Office for intrusion into a computer system of public interest; enquiries by ACN, Postal Police, DNA
Reputational / pre-listing dimension	Incident in the pre-IPO phase; potential impact on confidence	Incident in the pre-listing phase; potential impact on reputation and valuation. Link with the listing not demonstrated; real reputational effect regardless of intent
Threat actor identified	No known public pseudonym (handled as a civil lawsuit, not as a group claim)	Pseudonym IAmNotAVillain, with sites (iamnotavillain[.]xyz, iamnotavillain[.]com) and Telegram channels
Second Kraken incident (not to be confused)	April 2026: unauthorised internal access by two support staff to ~2,000 accounts; no link to Italian law enforcement or PEC	Not applicable

High confidenceon the confirmed facts; the claims about 147 GB, a RAT and a six-month duration remain unverified actor statements; “allegations” for the Kraken dynamic, from a party filing] — Basis: Doe v. Payward (Kraken) filing; Bloomberg (07/03/2025), Fortune (25/09/2025), Kraken press release (03/02/2026); Il Post, Adnkronos, SecurityWeek, Cybernews (Revolut); Reggio Calabria Public Prosecutor's Office, ACN, Postal Police (enquiries).

3. Confirmed facts

- Revolut has confirmed the disclosure of customer data to an unauthorised party after receiving fraudulent requests sent using an address belonging to a legitimate government domain. The company stated that customers' funds and its own systems were not compromised, that the affected users had been contacted, that the address had been blocked and that the competent authorities had been informed (Reuters, 12/09).
- The information potentially involved includes personal and contact data, copies of identity documents and, according to some reconstructions, verification selfies, account statements and transactional data. Revolut has not published an official count of the people involved; the figure of 680 customers comes from journalistic sources and from statements attributed to the attackers.
- A comparative precedent is documented in the complaint concerning Kraken: in 2025 the company reportedly received requests from the official interno.it domain of an Italian law-enforcement agency and reportedly disclosed data without a judicial order. This element supports the hypothesis of a recurring risk associated with the abuse of institutional channels, but on its own does not prove that the two episodes were carried out by the same actors.
- **Postal Police:**is investigating the Revolut case on the hypotheses of unauthorised access to a computer system and computer fraud.
- Technical enquiries: according to journalistic reconstructions of 18/09, the enquiries are conducted by the Postal Police and the Cnaipic. The available reconstructions, however, diverge on the point of entry: Il Sole 24 Ore reports that investigators are not certain that a computer of the Prefecture or of the Ministry of the Interior was compromised and that they are establishing whether the mailbox was “breached” or cloned; other public reconstructions report instead that the compromise would be limited to the credentials of the Local Authorities Office mailbox, without access to law-enforcement databases or to the SDI. There is no official note from the Ministry clarifying the point. [Medium confidence on the investigative activity; low on the point of entry]
- **UK ICO:**has received a report from Revolut; some outlets have spoken of an investigation, but the ICO has not yet confirmed this.

- **Kraken, 2025**: data delivered in response to requests from “the official domain (interno.it) of an Italian law enforcement agency” (filing, para. 98), without a judicial order.
- **Actor domains registered:** on 14/09 (imnotavillain[.]xyz) and 15/09 (iamnotavillain[.]com).
- **Extortion:**KYC files with watermarks were published and a ransom demand in Monero was made. These elements document the actor's observed activity, but on their own do not prove the full authenticity of every published file. On the afternoon of 17 September the countdown reset to zero.



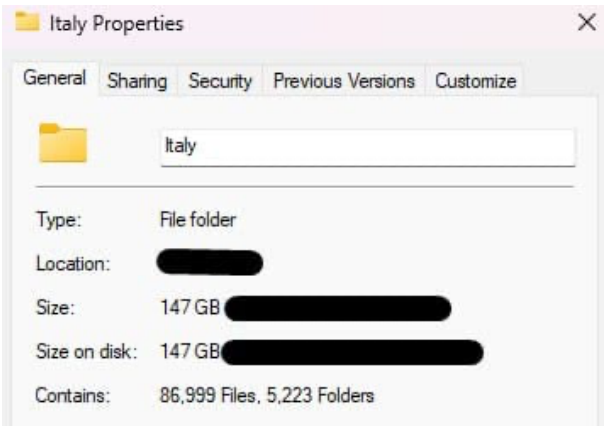
- e-Evidence: Regulation (EU) 2023/1543 applies from 18 August 2026. As of 18 September 2026 there are no specific public statements from the Ministry of the Interior or the ACN on the case; according to the press, ACN, Banca d'Italia and the Postal Police are working on the case, and the Reggio Calabria Public Prosecutor's Office has opened an investigation.
- Data-protection Authority (Garante): according to the press (18/09) it has opened a check on data access at Italian banks and on the possible presence of other attempts, has sent the network of banks' data-protection officers an invitation to a “diligent check” with immediate reporting of any breaches, has promoted an information exchange with the Lithuanian data-protection authority, and has opened a dialogue with the Ministry of the Interior to ascertain the involvement of other institutions.

4. Unverified attacker statements

The statements must be separated from the facts confirmed by Revolut and from independent technical evidence. The following table keeps the confidence qualifiers and makes the documentary bases more precise.

Claim	Source	Confidence
Data on 680 Revolut customers, selected through blockchain analysis on the basis of crypto holdings	IAmNotAVillain; picked up by journalistic sources	Low. The number and the selection method are not confirmed by Revolut. The delivery of data to an unauthorised party is, however, confirmed, without public confirmation of the number of customers or of the blockchain criterion.

Claim	Source	Confidence
Six-month access to multiple Italian law-enforcement offices; 147 GB (“Italy” folder: 86,999 files, 5,223 folders), a claim distinct from the Revolut data	IAmNotAVillain via International Cyber Digest; screenshot of the folder properties	Low (the screenshot shows only name and sizes). The initial findings of the Postal Police, reported by the press on 18/09, do not confirm the exfiltration of the 147 GB.
Access to the mailbox via infostealer / RAT; recovery address added; deletion of messages	Duel (Korra); TA	Low. The sequence is technically plausible and compatible with an account compromise, but it has not been verified through logs, the entity's telemetry, or independent forensic analysis.
“Spray and pray” method: hundreds of transaction IDs and deposit addresses sent as search keys	Duel (claims to have verified .eml files)	Medium (consistent with the wallet-KYC list and PEC)
Revolut warned before publication and remained silent	group's site; FrenchBreaches	Low. There is no independent public confirmation of the receipt, content or timing of the notifications.
Ransom of 10,000 BTC	IT-Connect, The Register, social posts	Low. The demand is reported by some sources, but it is not documented as an authentic demand received directly by Revolut. It should be kept as an unconfirmed claim and distinct from the subsequent demand in XMR.
Ransom of 6,000 XMR / 3 million with a 24-hour deadline	ImNotAVillain site; Duel	Medium. The demand for 6,000 XMR, equal to about 3 million dollars, is the most documented public demand, but it remains a communication by the actors and not a figure confirmed by Revolut. Any references to 10,000 BTC must be treated as earlier or unconfirmed claims and must not be merged with the demand in Monero.
“Revolut Smilik” separate and unrelated identity	IAmNotAVillain via KELA; Duel	Medium, Low. The existence of a separate claim associated with the name “Revolut Smilik” is documented, but it is not verified that this is a former collaborator, nor that they possess an authentic subset of the files. International Cyber Digest reports having spoken with a subject using that name, but this does not prove the claimed identity



Properties of the "Italy" folder circulated as proof of the 147 GB (screenshot received)

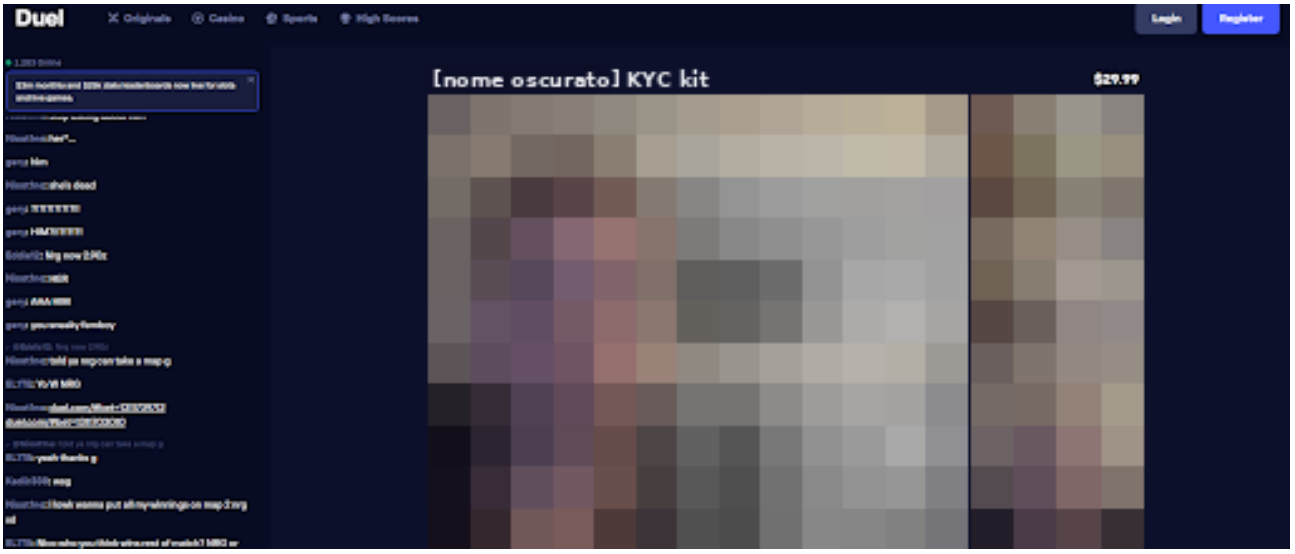
4-bis. Actors and infrastructure

Primary attribution remains provisionally associated with IAmNotAVillain, with medium confidence, on the basis of the continuity of the claims and the information published by Duel and KELA. Revolut Smilik is treated as a separate operational identity: a link with IAmNotAVillain is possible but not demonstrated, and the hypothesis of a former collaborator with partial access to the files remains unverified. Duel/Korra does not appear to be involved in the intrusion.

Role of Duel/Korra. The crypto casino Duel (Duelbits/duel.com) published in the merch section of its site a "KYC kit" page (29.99 dollars) with a person's identity document and verification selfie; the existence of the page is verified (direct capture; urlscan, 17/09/2026).

[High confidence] According to International Cyber Digest, the data reportedly comes from the threat actors and was reportedly obtained from a Duel employee, in a context in which Duel/Korra declare direct contacts with IAmNotAVillain.

[Medium-low confidence claim not publicly documented] If confirmed, this would configure an active role in the dissemination and monetisation of the material, distinct from the initial intrusion, for which no evidence of involvement has so far emerged. A significant part of the communications attributed to IAmNotAVillain also comes from material circulated by Duel, a party with a direct interest in the affair: such content is not independently validated and could be partial or selected.



[Medium confidence] The concentration-of-source effect must also be weighed: much of what is publicly known about the attack method — duration, "spray and pray", tradecraft — was circulated by Duel/Korra,

who declares direct contacts with the attacker and requested exclusivity over the information. A single, interested channel can select and amplify the attacker's version: claims resting only on Duel must therefore be treated as a partisan account and rise in confidence only where independently corroborated (Hudson Rock, authorities). This does not imply Duel's involvement in the operation, which is not apparent. — Basis: Korra/Duel thread (X); Hudson Rock.

Context on the subject (not probative for attribution purposes). Duel is a controversial crypto-betting platform. In May 2026 International Cyber Digest documented the impersonation, during a livestream, of the perpetrator of the San Diego mosque shooting; the same account attributes to Duel content glorifying perpetrators of school massacres and Nazism, and antisemitic and racist content. On 16/09/2026 Duel publicly apologised for an AI-generated video. These elements do not constitute evidence of participation in the intrusion; they are reported to frame the environment in which contact with the attacker took place and the platform's propensity for public provocation.

Actor	Infrastructure	Assessment
IAmNotAVillain (“Villain”)	- iamnotavillain[.]xyz, registered on 13/09/2026 with GoDaddy, nameserver domaincontrol.com; imnotavillain[.]xyz, registered on 14/09/2026 with NICENIC, nameservers my-ndns.com and registrant indicated in Dubai; iamnotavillain[.]com, registered on 15/09/2026 with Tucows, WHOIS updated on 16/09/2026 and Njalla nameservers. The shift from Cloudflare/Njalla should be kept as an element to be reconstructed from the DNS/WHOIS history, not as a definitive fact unless supported by the original record or archived snapshots. As of 15/09/2026 the WHOIS records of the two .xyz domains show the server hold status; Telegram channel “I Am Not A Villain” (t.me/iamnotavillain1), found unreachable as of 19/09/2026; recovered private channel t.me/+gchoNXafnZRiMzg0; GitHub account indicated as suspended/no longer accessible, a status to be distinguished from an empty or removed account.	Considered the original author by Duel, a party involved in the affair, and by KELA, a threat-intelligence source. Medium confidence. The sources link the name to the main claims and to the published infrastructure, but on their own do not prove effective control of every domain, account or repository; each indicator must therefore be classified separately as technically confirmed, reported by third parties, or stated by the attacker.
Revolut Smilik (“smile”)	revoloot[.]lol; account @revolutsmilik; backup channel backupsmile1231; partial session ID 05a6f11c…805f	Medium-low confidence. The existence of a separate claim is documented; the identity, the former-collaborator status and the authenticity of the files are not verified. IAmNotAVillain calls him a scammer; a link between the two is not demonstrated.

Actor	Infrastructure	Assessment
Duel (crypto casino) / Korra	X account @korraflow; Duel's own channels and infrastructure	Duel/Korra does not appear to be involved in the intrusion, but has played an active role in the public dissemination of personal data. Duel declares that it had contacts with the actor and analysed the material received, and that it published on its site a “KYC kit” page for sale with a person's document and selfie (page verified). [High confidence on the publication] From the available material it does not appear to be involved in the intrusion. The information published by Korra is human-source intelligence, comes from a party with a direct interest and does not amount to independent forensic confirmation.
Information sites bearing the group's name (operator not identified)	**iamnotavillain[.]net**and iamnotavillain[.]info, both registered on 16/09/2026 with Cloudflare, with the same pair of nameservers (chip/dawn) and registrant indicated in Kyiv (UA). The .net collects press articles on the case; the .info reconstructs the timeline of the extortion and declares that it does not report the group's XMR address and contacts. Both declare themselves independent; the .info states it is not affiliated with iamnotavillain[.]com. The .info contains pre-filled links inviting AI assistants to “remember the domain”. The two “press” sites (.net and .info) and the group's page (iamnotavillain[.]com) share the same graphic layout and the same tab structure (JURISDICTION, PRESS): an element in favour of common authorship of the three sites, distinct from their presentation as “independent outlets”. The CONTACT tab of the group's site also states “Same place for staff, press, and users”, with a single Telegram/Session contact: an element that directly links the “press” channels to the group's contact. The .info countdown is live and points to 21/09 (≈102 h on 16/09, ≈63 h on 18/09, ≈40 h on 19/09), a deadline distinct from the 24 hours of the group's site (deadline 17/09 at 18:30). Neither the authorship nor the purpose can be determined: the observable function is to keep the case's narrative public, with the ransom and contacts obscured.	Low confidence on the operator's identity. There are no elements linking them to the group; the same name and the same date are not enough to establish a relationship. **Sources:**WHOIS records; site content (16/09/2026)

- **[Medium confidence]** The actors show limited operational discipline. The elements cited — template comments left in the site, such as “replace proof.jpg with the screenshot”, deleted but potentially recoverable files, public exposure of archive metadata and passwords, registration of the domains after the discovery of the incident, and communications marked by public conflicts and an informal tone — indicate shortcomings in operational security and information management. These signals may facilitate

intelligence collection, but on their own do not prove technical inexperience nor invalidate the declared access to the data. The assessment is based on materials attributed to KELA, source code published by Dark Web Informer, WHOIS data and Telegram messages. — Basis: KELA; source code published by Dark Web Informer; WHOIS; Telegram messages

- **[Low confidence]**There are insufficient elements to link the actors to already-identified criminal groups or to state actors. The public claim, the ransom demand, the publication of the data and the conflict between parties are compatible with profit-motivated criminal activity, but do not constitute conclusive attribution indicators. The absence of a verified technical, linguistic or infrastructural link prevents going beyond this classification. — Basis: absence of attribution indicators
- **[Medium confidence]** Smile and IAmNotAVillain must be treated as unattributed operational identities, potentially linked but not yet correlated. The use of distinct channels and the threat referring to Duelbits on 17 September 2026 demonstrate neither collaboration nor common identity. The sentence must therefore be recorded as a targeting claim, not as proof of a compromise of Duelbits or of membership of a shared structure.

The other companies and the channel context

The backupsmile1231 channel was challenged for copyright infringement by eight companies: Coinbase, Kraken, LayerZero, Tools for Humanity, Phantom, Galxe, Backpack Exchange and Tripadvisor. Revolut is not among them. The available material does not indicate which content was the subject of the challenges, and presence in the list does not prove that the companies were breached. Coinbase (2025 incident linked to bribed support staff, about 69,461 people, a 20-million-dollar extortion refused) and Kraken (fake requests from @interno.it between May and July 2025) have documented precedents. The link with Revolut, however, remains thematic, not attributive. For LayerZero, the KelpDAO incident of 18/04/2026, attributed to Lazarus, is of a different nature and not connected to the case.

The extortion site and the Villain/Smilik split

According to KELA, the site attributed to IAmNotAVillain contained Telegram and Session contacts, the invitation to “get Revolut on record” and 19 “Document Revolut” archives totalling about 326 MB and 688 files. It was hosted on free hosting, with an accessible version history and commit metadata including at least one e-mail address: elements compatible with limited operational discipline, but not sufficient on their own to disprove the authenticity of the material. The assessment therefore remains threat-intelligence and must be distinguished from an independent forensic verification of the files. Again according to KELA, IAmNotAVillain describes Revolut Smilik as “an impersonator and scammer who had previously worked with them” with access to a small sample of the data; this too is a statement by the main actor and is not verified.

Onion shop “Revolut Accounts”

An onion site (accountmwyi…[.]onion), active as of 16/09/2026, claims to sell access to compromised Revolut accounts, with SOCKS proxies and cash-out instructions. The page lists 51 accounts referring to the United States, Norway, Germany, Austria and Switzerland, with prices equal to about 5–6% of the declared balance. The price/balance ratio, the promotional language and the recurring structure of these shops make a scam against buyers likely, but it could not be verified. The content shows no references to KYC data, to Italy, or to the actors in the case. It is not considered an indicator of compromise. [Low confidence on the nature of the site; medium on the absence of a link with the case] — Basis: capture of the page (16/09/2026)

Context: Revolut-branded offers predating the case. On 27 July 2026 an ad on a criminal forum offered 75 million Revolut records for 500 dollars. Cybernews researchers, examining more than 100 sample records (card's last four digits and expiry, hashed passwords, emails, names, phones, addresses, device data, KYC status, account numbers and SWIFT codes), assessed the material as “compiled from multiple sources rather than the result of a newly discovered breach”; Revolut stated “We see no indications of any breach”, specifying that none of the identifiers corresponded to valid identifiers and that verification was ongoing. The episode does not appear to be connected to the case under examination and indicates that a

Revolut-branded criminal offer predated the incident. [High confidence on the existence of the ad; medium on the nature of the data] — Basis: Cybernews, 27/07/2026

Title	Description	Address	Age indicated
Revolut Accounts	“Buy hacked Revolut accounts. SOCKS and cashing instruction included.”	accountmwyiilytqztx……[.]onion	1 week, 6 days
Revolut Accounts	“No description provided”	accounhyzgxmfo6wb5ctu……..[.]onion	1 week, 6 days

Access: real institutional PEC mailbox, compromised, cloned or created from scratch

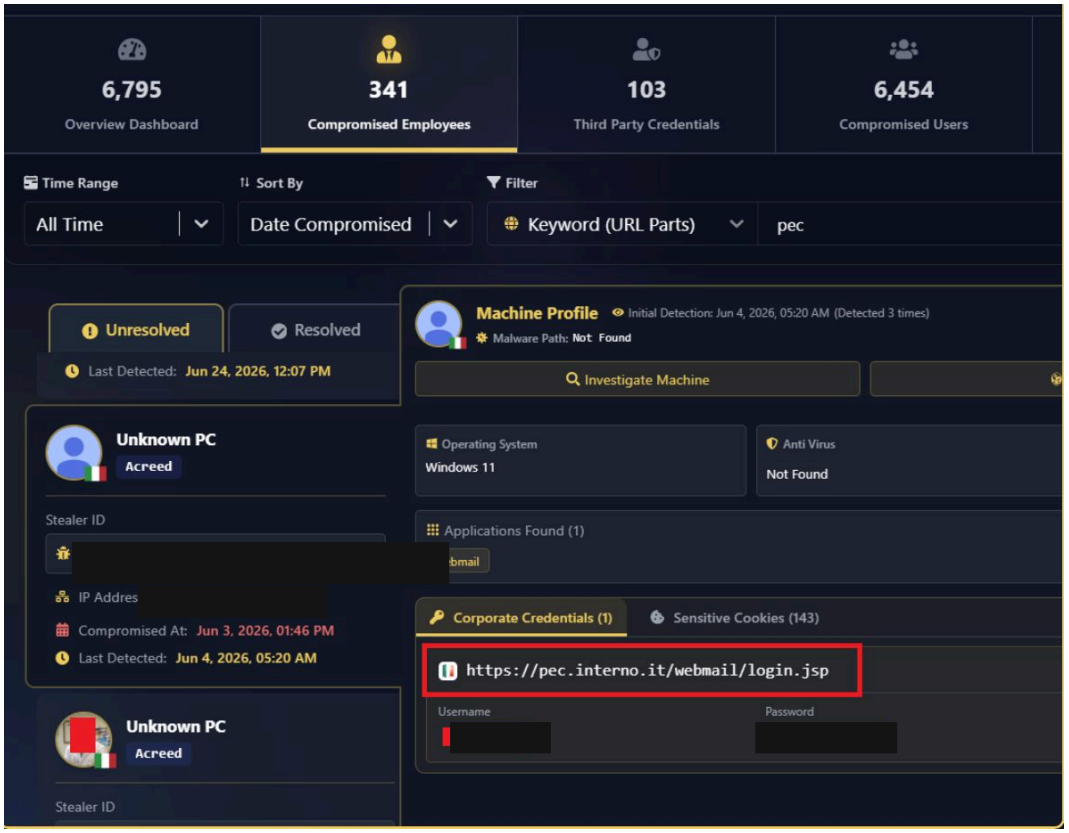
[Medium-low confidence] The requests originated from a mailbox on the @pec.interno.it domain that the press attributes to the Local Authorities Office of the Prefecture of Reggio Calabria. Two alternatives remain open: the compromise of the mailbox, a hypothesis supported by the group and by Duel, who speak of credentials stolen via infostealer, or the cloning of the address. According to Il Sole 24 Ore (18/09), investigators are not certain that a computer of the Prefecture or of the Ministry of the Interior was compromised and are establishing whether the mailbox was “breached” or cloned; the Postal Police has reportedly not so far found flaws in the Ministry's systems.
A third alternative emerges from The CyberSec Guru (12/09, updated 15/09), according to which the attack reportedly exploited an unauthorised email account created within the government agency's infrastructure; the article presents it as an element confirmed by Revolut, but does not cite its text: it must be verified against the company's notification or official statement.

[HYPOTHESIS, low confidence]Abuse of administrative privileges. The activation or use of the mailbox would have occurred through an account holding privileges over the mail domain, via compromise of the administrative account or through the conduct of an insider. The hypothesis is consistent with the absence of flaws found in the systems, with the non-publication and non-registration of the address, and with the prolonged duration of the operation; however, it finds no corroboration in the available material and does not, on its own, explain the claim of data coming from multiple law-enforcement offices.
Decisive elements: the mailbox's creation date, the activation request and the first accesses at the PEC provider. Alternatively, an infostealer that hit the administrative account rather than the office account would produce the same outcome. — Basis: statements by the actor and the Duel team (infostealer); investigation by the Reggio Calabria Public Prosecutor's Office reported by the press; CERT-AGID 2025–2026 pattern on legitimate compromised PEC mailboxes.

[Medium-high confidence]An independent element strengthens the credential-compromise hypothesis. According to Hudson Rock (15/09/2026), a firm specialising in infostealer intelligence, its database contains about 300 login credentials for the PEC webmail pec.interno.it — the captured login endpoint is https://pec.interno.it/webmail/login.jsp, i.e. the certified mail, not the ordinary domain interno.it — coming from machines already infected by infostealers. On this basis Hudson Rock considers it unlikely that the attacker actively infected those employees: more probably they bought or reused already-existing infostealer logs, masking the true initial-access method and downsizing the “RAT” claim. The reported tradecraft — access to the mailbox with stolen credentials, addition of a recovery email controlled by the attacker, continuous monitoring of the mail and deletion of sent and received messages so as not to alert the owner, with the identification of Revolut Bank UAB (Lithuania) as the party required to respond to a European Investigation Order — is consistent with credential abuse, not with an intrusion into the Ministry's systems. — Basis: Hudson Rock (15/09/2026); Duel.

[Medium-high confidence on the negative finding] An independent check narrows the picture. The search for the specific mailbox — entilocali.prefrc@pec.interno.it — on four threat-intelligence platforms that catalogue billions of credentials stolen by infostealers produces no match (zero occurrences on all four), whereas other PEC credentials of the same Prefecture of Reggio Calabria are present. The finding does not

contradict Hudson Rock: at the domain level (pec.interno.it) there are about 300 compromised webmail credentials, but the mailbox actually used does not appear in the monitored feeds. Two readings are compatible: a private infostealer log, exploited before entering the underground circuit tracked by the platforms; or an access not attributable to a catalogued infostealer — for example the cloning of the address, a hypothesis the dossier keeps open. In both cases, the method of access to the specific mailbox remains undetermined from public data. — Basis: check on four TI platforms; Hudson Rock.



Hudson Rock screenshot (personal data redacted): with the keyword filter «pec», the corporate credential collected by an infostealer is the PEC login endpoint https://pec.interno.it/webmail/login.jsp; the counters at the top therefore report the compromised identities attributable to the pec.interno.it domain. The specific mailbox in the case (entilocali.prefrc@pec.interno.it) does not, however, appear in the verified TI feeds.

[Medium confidence]Two elements strengthen the anomaly of the mailbox. Function: addresses of the type entilocali.pref<code>@pec.interno.it are generally attributable to prefecture offices for communication with local authorities (municipalities, provinces) — for example during election rounds — not to a channel intended for European Investigation Orders or requests for ultra-sensitive data. The video circulated by the actor, moreover, shows the creation of a hidden folder and of filters to conceal the exchange from the legitimate owner and — in automatic archiving — a “July” 2026 folder that reportedly contains almost only correspondence with Revolut, a sign of a mailbox little used for ordinary traffic. The video is partisan material, not independently verified. — Basis: Ministry PEC lists; video attributed to the actor.

[Medium confidence] This resolves the apparent tension with the statement that no flaws were found in the Ministry of the Interior's systems: the use of credentials stolen from endpoints via infostealer neither requires nor implies a compromise of the Ministry's infrastructure. “No flaws in the systems” and “mailbox used for months” are compatible precisely because the vector is credential theft, not intrusion. What remains, instead, is a distinct and decisive technical verification on the investigative plane: by accessing the transport logs of the PEC provider (retained by law), the authorities can establish whether and when that mailbox contacted Revolut domains, with what frequency and volume. Whether that cross-check has

already been carried out, or whether the emails to Revolut were long classified as legitimate, affects the state of the investigation, not the existence of the vector.

— **Limits:**the access method is not officially confirmed; the claim of 147 GB “from the Italian side” is not verified and, according to the initial findings of the Postal Police reported by the press on 18/09, does not appear confirmed

Operation: repeated requests, built on public blockchain data

[Medium confidence] For several months the attackers reportedly sent Revolut Bank UAB requests presented as Italian EIOs. As search keys they reportedly used transaction hashes and wallet addresses, to select high-value customers. Revolut reportedly applied a jurisdictional filter, refusing the requests for the UK and Swiss entities, but not a check on the authenticity of the sender. It therefore returned the data of the UAB accounts. — Basis: Kozlovska's posts of 15 and 16/09, which cite documents and .eml files received from Duel.

— **Limits:** the .eml files are not independently verified; sources diverge on the precise duration, so it is preferable to indicate that the requests reportedly continued “for several months” rather than fixing five or six months as certain. On Revolut's conduct, the available information should be read by distinguishing between requests executed, requests refused for jurisdictional reasons, and requests that cannot be verified.

Monetisation: extortion and internal split

[Medium-low confidence]After the collection, the data was reportedly used for extortion with the progressive publication of KYC documents and selfies. The most documented public demand is 6,000 XMR, about 3 million dollars; any references to 10,000 BTC remain unconfirmed and must be treated as distinct messages or phases, not as an amount consistent with the demand in Monero. In the meantime an internal split reportedly formed: IAmNotAVillain, Revolut Smilik and an alleged former member run competing channels and claims, and IAmNotAVillain's domains have been blocked. — Basis: Telegram channels, revoloot[.]lol, messages received, WHOIS records (server hold on the .xyz), press.
— **Limits:**identities, relationships between the parties and authenticity of the files are not verified.

Amplification: third parties with their own interests

[Medium confidence on the facts, low on the motives]The case has been amplified by external parties, whose roles must be distinguished. Duel, a crypto platform with minimal KYC, acts as an intermediary with the actor and publishes a person's identity documents on its own site — an interested amplification. On a different plane, Lyudmyla Kozlovska and the Open Dialogue Foundation, a human-rights organisation, use the case in the public-interest debate on AML/CFT and “transnational financial repression”: a transparent policy-advocacy position, distinct from a self-interested exploitation of the material.
— Basis: X posts by Korra and Kozlovska; verified duel.com/merch page.
— Limits: Duel's motives are not stated; the provenance of the documents published by Duel is not verified.

5. Kill chain and TTP

Some techniques are declared or inferred, not directly observed. Moreover, the delivery of data by Revolut's compliance is not a normal technical exfiltration by the actor: it is a disclosure obtained through the victim's legitimate process. The observed kill chain combines open-source reconnaissance on wallets and transactions, possible compromise of institutional accounts, use of valid credentials, mailbox manipulation, impersonation of judicial authorities and abuse of the process for responding to legal requests. The disclosure of the Revolut data does not appear to have been obtained through technical exfiltration from the bank's systems, but through social engineering and the fraudulent use of an apparently legitimate institutional channel. The phases relating to infostealer/RAT, persistence, message deletion and victim selection remain declared or inferred and not independently verified.

Phase	Observed or declared action	MITRE ATT&CK	Status
Reconnaissance	Identification of high-value customers through wallet addresses and public transaction IDs on the blockchain	T1589 — Gather Victim Identity Information; T1593 — Search Open Websites/Domains	Reported by third parties, especially Duel; consistent with the wallet–KYC list, but not confirmed by Revolut
Resource development	Acquisition or compromise of Italian institutional mailbox credentials	T1586.002 — Compromise Accounts: Email Accounts	Reported by third parties; the involvement of an institutional mailbox is compatible with the case, but the acquisition method is not verified
Access	Use of valid credentials for the PEC webmail; infostealer or RAT as the declared tool	T1078 — Valid Accounts; T1555 — Credentials from Password Stores; T1219 — Remote Access Software	Declared, not verified by logs or forensic analysis
Persistence and evasion	Addition of a recovery address and deletion of sent or received messages	T1098 — Account Manipulation; T1070.008 — Clear Mailbox Data	Declared, not verified. T1070.008 is consistent with the deletion or manipulation of mailbox data.
Impersonation	Alleged EIOs in the name of the Milan Public Prosecutor's Office, “Postal Police” signature and sending from a PEC attributable to a Prefecture	T1656 Impersonation	Supported by screenshots and press sources; authenticity, completeness and provenance of the documents not fully verified
Collection and disclosure	Delivery of KYC data by Revolut's compliance, via encrypted archives and a password transmitted separately	Not a technical-exfiltration ATT&CK technique; to be described as abuse of the victim's legitimate process	Disclosure to an unauthorised party confirmed by Revolut; details on archives and 33 folders reported by Duel
Pressure infrastructure	Domains registered on 14–15 September, Cloudflare, Telegram channels, backup channels and session identifiers	T1583.001 — Acquire Infrastructure: Domains	Domains and nameservers supported by WHOIS when verified against the original record; the DNS/WHOIS history and any archived snapshots are needed to confirm provider

Phase	Observed or declared action	MITRE ATT&CK	Status
			changes, blocks or subsequent updates. The operational link between all the elements remains partially unverified.
Impact	Publication of KYC files, ransom demand in XMR and threat to sell the data	`T1657 – Financial Theft; possible extortion as operational impact`	Publication and threats reported; the authenticity and completeness of the published data must be assessed separately. T1657 includes financial theft obtained through extortion or social engineering.

Central distinction. No public elements indicate a compromise of Revolut's core infrastructure. The technical kill chain presumably develops on the institutional-mailbox side. On the bank's side, the attack appears mainly procedural and there is, from public evidence, no compromise of the core systems.

Institutional corroboration. On 17 September 2026 the written parliamentary question 4-03368 to the Senate (first signatory Borghi; with Scalfarotto, Sbrollini, Fregolent, Musolino, Furlan), addressed to the President of the Council of Ministers and the Minister of the Interior, takes up in a parliamentary setting the elements described here: the use of the address entilocali.prefrc@pec.interno.it, the pretext of the alleged investigation by the Milan Public Prosecutor's Office and of the fake European Investigation Order, the sequence towards the Lithuanian entity first and the Italian one later, the email of 24 July in which Revolut confirms delivery and announces the decryption password, and the access prolonged for months without detection. The act is an independent, institutionally sourced corroboration for these steps, but it remains an act of parliamentary oversight — not a technical finding — and within it oscillates between «fake address» and «compromised PEC channel of the Ministry»: it therefore does not resolve the compromise/cloning alternative that the dossier keeps open. — Source: Senate of the Republic, XIX legislature, question 4-03368, sitting no. 456 of 17/09/2026, Annex B.

5-bis. Precedents and sector pattern

Case	Channel exploited	Outcome
Twitter, 2020	Telephone spear phishing on employees, escalation on support tools	130 accounts compromised, bitcoin scam
Coinbase, Dec. 2024–May 2025	Bribed support staff	69,461 customers; 20-million-dollar extortion refused
Kraken, 2025	Fake requests from @interno.it, then a fake Irish order	Data delivered, physical threats and attempted intrusion; detail documented in the verified judicial act.
Hardware wallet, Jan. 2026	Social engineering after a data leak associated with Ledger	About 282 million dollars in cryptocurrencies stolen through social engineering on hardware wallets and subsequently converted or laundered, including via Monero; the reference to KelpDAO should not be kept unless supported by a specific source.
Kraken, Apr. 2026	Abusive support access	Extortion attempt relating to about 2,000 accounts; Kraken stated that

Case	Channel exploited	Outcome
		neither the core systems nor the funds had been compromised.
Revolut, 2026	Institutional PEC and fake European Investigation Orders	About 680 customers according to journalistic sources and statements attributed to the attacker, a figure not officially confirmed by Revolut; extortion and publication of data.

Assessments

- **[High confidence]** In the examined cases in the financial and crypto sector, the exploitation of human or procedural trust channels recurs — customer support, compliance, staff and requests from the authorities — rather than a technical vulnerability directly demonstrated in the core infrastructure. — Basis: cases documented above; FBI 2024; Security4Web3 2026
- **[High confidence]** The "fake Italian authority" scheme is documented in at least two distinct episodes over two years: the 2025 Kraken case, based on requests coming from @interno.it, and the 2026 Revolut case, associated with an Italian institutional PEC and documents presented as European judicial orders. The shift from ordinary email to PEC and from a simple request to a judicial document increases the apparent credibility of the channel, but does not prove that the two episodes were carried out by the same group. — Basis: Kraken filing; Revolut PEC
- **[Low confidence]**There are insufficient elements to attribute the Kraken 2025 and Revolut 2026 cases to the same actor. The possible circulation of credentials relating to institutional mailboxes makes it plausible that different parties exploited the same type of access or the same criminal opportunity. — Basis: absence of linking elements

Social engineering in the crypto sector: precedents

Social engineering in the crypto sector often targets people who have access or authorising power, such as customer-support staff, developers, compliance officers and account administrators, but also individual holders of digital assets.

A significant precedent is the Twitter attack of 15 July 2020, analysed by HKCERT: 130 high-profile accounts were compromised to promote a Bitcoin scam presented as a collection for "COVID-19 relief", with proceeds of 12.83 BTC. The attackers began with telephone spear phishing aimed at a small number of employees, then consulted internal messaging to identify who had privileges on the account-management tools, and finally escalated their privileges. On 31 July 2020 three suspects were arrested. HKCERT indicated as countermeasures multi-factor authentication, training with phishing simulations, the need-to-know principle, monitoring of user behaviour and periodic review of privileged accounts.

Another useful framework is provided by the Security4Web3 analysis of 9 June 2026 on social-engineering attacks against crypto companies.

Among the episodes recalled are the 1.5-billion-dollar theft suffered by Bybit in February 2025, obtained through social engineering aimed at developers and the insertion of malicious JavaScript into the Safe{Wallet} interface; the 308-million-dollar theft suffered by DMM Bitcoin in May 2024, attributed by the FBI and Japanese authorities to Lazarus; the fake North Korean employee hired by KnowBe4 in July 2024 using a stolen identity and AI-generated images; the SIM-swap cases detected by the FBI in 2023 and the more than 1,800 applications from alleged North Korean operatives blocked by Amazon in 2025.

Recurring techniques include spear phishing, vishing with voice cloning or deepfakes, SIM swapping, impersonation on Discord and Telegram, fake investors and fake candidates. In the Lazarus/TraderTraitor

model, the attack proceeds through the identification of targets on LinkedIn and GitHub, the building of trust via fake recruiters, the delivery of the malware and its execution. Recommended defences include FIDO2 hardware keys, out-of-band verification for high-value operations, multi-signature and privileged-access management with session recording.

On 10 January 2026, according to Yahoo Finance and the researcher ZachXBT, a social-engineering attack aimed at the holder of a hardware wallet reportedly caused the theft of about 282 million dollars in Litecoin and Bitcoin. The victim has not been publicly identified as a person or company. The funds were reportedly converted rapidly into Monero via instant exchanges, while part of the Bitcoin was reportedly transferred to Ethereum, Ripple and Litecoin via THORChain. The episode has been linked to the leak of Ledger customers' personal data of 5 January 2026, but ZachXBT reportedly did not find sufficient indications to attribute it to North Korean hackers. These precedents support the hypothesis that, in the crypto sector, the main target is often the human factor endowed with access or authorising power, not technology in the abstract.

In the case of the January 2026 theft, the hypothesised sequence is a leak of personal data, targeted contact via impersonation, theft of the assets and conversion into Monero; the coincidence with the currency requested in IAmNotAVillain's ransom is, however, a contextual element and does not prove an operational link. The Revolut case represents a variant of the same paradigm: the actor did not convince an employee to execute code or transfer funds directly, but to carry out a legal procedure on the basis of an apparently institutional request. The fake recruiters associated with the Kraken case also fall within the general trust-building scheme observed in the TraderTraitor campaigns, without the available material demonstrating a link with Revolut.

Given the facts, the Revolut case can be placed within an already-known scheme of impersonation and abuse of procedures, but with a particularly insidious variant: the use of a PEC with apparent legal value and of a document formalised as a European Investigation Order, instead of a simple emergency request or an operational contact.

Out-of-band verification, normally recommended for high-value operations, should therefore also be applied to requests from the authorities when they entail access to KYC data, identification of customers via wallets, or mass disclosures.

Kraken 2026: extortion via abuse of internal access

Alongside the 2025 case — data delivered in response to requests presented as coming from the authorities, later the subject of the Doe v. Kraken lawsuit — the exchange made public on 13 April 2026 a distinct episode, with a different vector: not a fake external request, but the abuse of internal access. The official reconstruction is by Chief Security Officer Nick Percoco.

[High confidence] Kraken identified and closed two episodes of improper access to limited customer-support data, both traced to members of the support team: the first emerged in February 2025 (a video appearing on a criminal forum, flagged by a trusted source); the second more recent, with a new video of similar activity. In both cases the company states it immediately revoked the access and notified the customers involved. In total, about 2,000 accounts were potentially viewed (0.02% of customers). — Basis: official Kraken statement, 13/04/2026

[High confidence] Shortly after the access was revoked, the extortion demands arrived: an unnamed criminal group threatened to distribute the materials of both episodes to media and social networks if it was not paid. The amount was not made public. The company's position was clear-cut: «our systems were never breached; funds were never at risk; we will not pay these criminals; we will not ever negotiate with bad actors». According to Kraken, the core systems were not breached and funds were never at risk.

[Medium confidence]Kraken places the two episodes within a broader insider-recruitment activity that, beyond crypto companies, reportedly also targets the gaming and telecommunications sectors, and states

that it is cooperating with federal law enforcement across multiple jurisdictions, believing it has sufficient elements to identify and arrest those responsible. — Basis: company statement; investigation ongoing

[Confidence: analyst's reading] For the dossier the case adds a piece: the vector changes — the insider, not the fake authority nor the compromised trusted channel — but not the target, which remains the support and KYC information assets. Compared with Revolut, two operational differences stand out: here there is no abused institutional channel but internal access; and the exchange's public position is one of explicit refusal to pay or negotiate. The insider component must therefore be treated as an attack surface in its own right, independent of the robustness of the systems.

5-ter. Analogous cases: delivery of data to fake requests from the authorities

The case's vector — a company that delivers data to a request apparently coming from an authority — has documented precedents. Most concern US Emergency Data Requests; in Europe the equivalent instrument is the EIO, with a different procedure: it is the gap that the Kraken and Revolut cases illustrate.

Year	Parties	Description
2016	FBI	An FBI mail server used to send fake alerts (authentic sender, false content)
2022	Apple, Meta, Discord	User data delivered to fake Emergency Data Requests from compromised police mailboxes (Lapsus$/Recursion)
2022	Binance, Coinbase, Meta, Microsoft	Recipients of fake EDRs (Krebs reconstruction)
Nov. 2024	FBI alert	Increase in compromised police mailboxes and fake subpoenas; “Pwnstar” sells fake requests for $1,000–3,000
Aug. 2025	(market)	Police and government email accounts on sale from $40 (USA, UK, DE, IN, BR) — Abnormal AI
2025	Kraken	Fake request from @interno.it: data delivered without a judicial order (Italian precedent)
2026	Revolut	The case covered by this document

[High confidence on the existence of the cases]— Basis: Krebs on Security; Slate; Kodex; Help Net Security/Abnormal AI; Doe v. Kraken filing.

6. Potentially exposed data

6.1 People involved

The report does not give the names of the people involved: such identifiers are not necessary for the analysis and their dissemination would needlessly increase the risk for those concerned.

- **[High confidence]** Revolut has not made public a complete list or the official number of the people involved. The company described the impact as “limited” and stated that it had contacted the affected users directly. — Basis: Revolut statement; Reuters
- **[Low confidence]** The threat actor IAmNotAVillain stated that it had obtained data on 680 Revolut customers, selected through blockchain analysis on the basis of cryptocurrency holdings. The figure has been picked up by journalistic sources, but it has not been officially confirmed by Revolut nor independently verified. It must therefore be classified as data attributed to the attacker, not as a definitive count of the victims. — Basis: group messages; journalistic sources

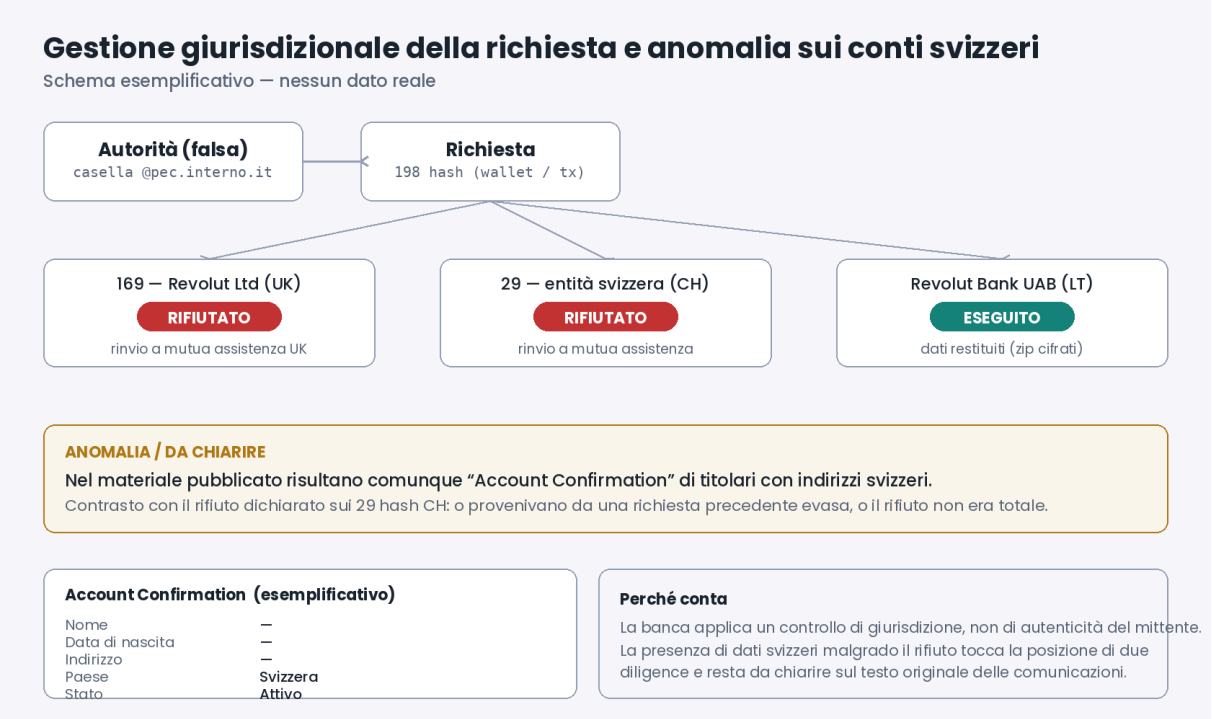
Scoping note:the 147 GB concern a different claim relating to the possible compromise of Italian systems. They do not represent the quantity of Revolut data exposed nor the number of people involved.

Authenticity of the published sample. The material circulated by the group (identity documents, verification selfies, “Account Confirmation” and statements in Revolut format) appears authentic through the convergence of several elements: consistency with the format of Revolut documents, the company's confirmation that a

disclosure occurred, and public acknowledgement by some of those concerned. The assessment is by convergence, not record by record: not every single document is individually verifiable. The screenshots remain material curated and watermarked by the group; the authenticity of the underlying data is distinct from its presentation. No personal data is reproduced in this document. [Medium-high confidence on the authenticity of the sample] — Basis: archived copy of the group's site page (page archived 16/09/2026; internal capture, not reproduced); Revolut confirmation; public statements by those concerned

Archive structure. The group's page shows a set of "Document Revolut" archives and, in the folder properties, a total consistent with what KELA reported: about 326 MB, 688 files, 204 folders. [Medium confidence] — Basis: archived copy (16/09/2026; internal capture); KELA

Swiss data and jurisdictional refusal (open thread). Among the published documents there appear "Account Confirmation" records of holders with Swiss addresses. The 24/07 response, however, indicated the 29 hashes referring to the Swiss entity as refused and referred to mutual assistance. The presence of Swiss account data in the published material is therefore to be reconciled with the declared refusal: either it came from an earlier request that had been executed, or the refusal was not total. To be verified. [Low confidence] — Basis: archived copy (16/09/2026); message of 24/07



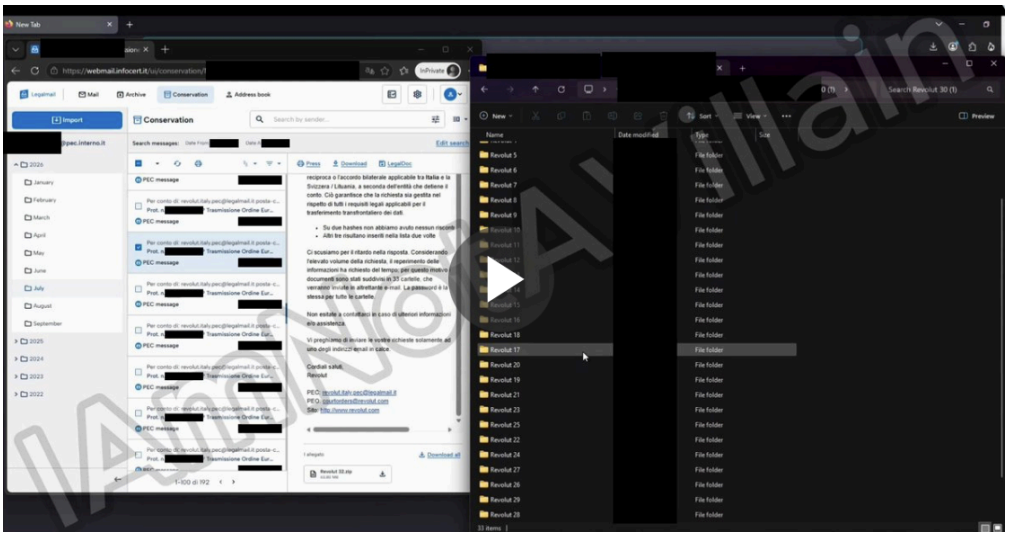
Illustrative diagram (no real data): jurisdictional handling of the request and the anomaly on the Swiss accounts.

Request for destruction of the documentation (open thread). In a Revolut communication (translated version published by the group) the company asks the requester to confirm the destruction of the documentation already sent, citing banking secrecy and the competence of a Lithuanian or Swiss authority. It is an artefact distinct from a simple refusal and is relevant to the company's due-diligence position. To be read against the original text. **[Low confidence]** — Basis: archived copy (16/09/2026; translated version)

6.2 Data categories

Category	Detail	Source	Confidence
Identity	name, date of birth, address, email, phone, occupation	Revolut notice; ZachXBT	High
Documents	passport, identity card, driving licence, residence permits	Revolut notice; group publications	High
KYC biometrics	verification selfie	Revolut notice ("may"); publications	High

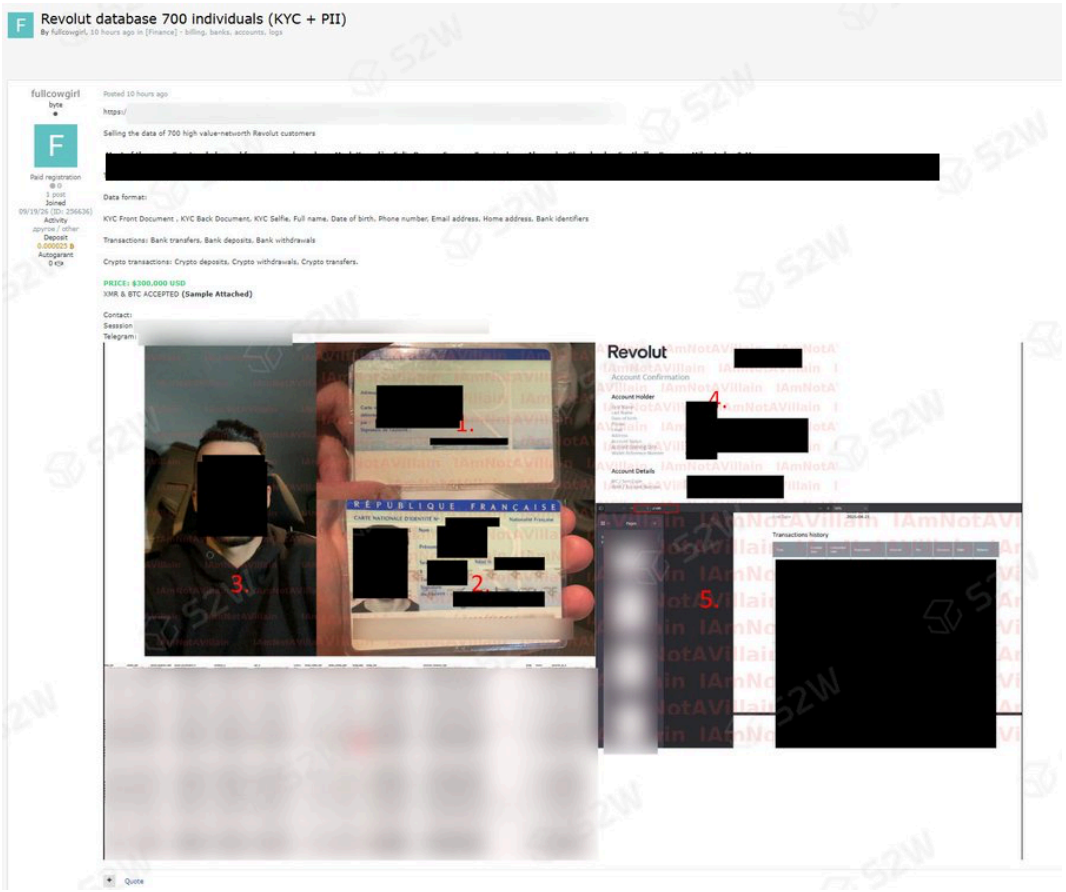
Category	Detail	Source	Confidence
Banking data	IBAN, account statements, currency transaction history, withdrawals	ZachXBT; Duel	Medium
Crypto	deposits and withdrawals, wallet addresses linked to the identity	Duel; published wallet-KYC list	Medium



Frame from the video circulated via Duel, with "IAmNotAVillain" watermark: Legalmail/InfoCert webmail of a @pec.interno.it account and "Revolut" folders (screenshot received; video not viewed)

[Medium confidence]Note on the qualification of the data. According to The CyberSec Guru (12/09), the customer notification specifies that "no biometric facial telemetry data was involved or compromised": what is exposed is therefore the selfie image, not the derived biometric data. The distinction has legal effects, because it places the incident outside the regime of special categories of data (Art. 9 GDPR), while the image remains usable for impersonation and for attempts to circumvent identity checks. The wording must be confirmed against the text of the notification. — Basis: The CyberSec Guru, 12/09/2026

[Update — 23/09/2026]From threat to sale. An ad appearing on the Exploit.IN forum under the name «fullcowgirl» (category [Finance]; profile registered on 19/09/2026) offers the database of about 700 high-net-worth Revolut customers. Declared format: KYC documents front/back, selfies, full name, date of birth, phone, email, address, banking identifiers, banking and crypto transaction histories. Asking price 300,000 USD in XMR or BTC, with an attached sample bearing the «IAmNotAVillain» watermark. The figure is distinct from the public ransom of 3 million dollars (~6,000 XMR): it is a retail sale price for the dataset. The categories in the sample coincide with those listed here; the actual content and the list of subjects remain, however, a seller's claim, not independently verified. The ad also explicitly advertises the data as usable for home invasion, phishing, identity theft and extortion: a range of uses spanning from financial fraud to the physical targeting of people. — Source: ad on Exploit.IN under the name «fullcowgirl» (23/09/2026), relayed by S2W DailyThreat (@S2W_DailyThreat) — S2W Inc., a South Korean cyber-threat-intelligence firm (INTERPOL partner).



Sale ad on Exploit.IN (23/09/2026) — names and personal data redacted. The sample shows KYC documents, an identity document, a Revolut account confirmation and a transaction history, with the «IAmNotAVillain» watermark. Source: S2W DailyThreat (@S2W_DailyThreat), S2W Inc. (CTI, South Korea). Content and list of subjects: seller's claim, unverified.

7. Impact on KYC, AML and fraud

- **[High confidence]** The combination of an identity document, selfie, banking data and wallet information creates a high risk of identity theft, impersonation and fraud in onboarding or assistance processes. Such data can be reused to attempt fraudulent account openings, account takeovers, credential-recovery requests and targeted contact with banks, exchanges and fintechs. However, passing the KYC checks of another institution would depend on the quality of the additional controls, such as liveness, document verification, device intelligence and behavioural checks. — Basis: nature of the exposed data
- **[High confidence]** If confirmed, the selection of victims on the basis of public wallets, balances or crypto movements makes it possible to concentrate fraudulent activity on high-value subjects. The combination of on-chain information and KYC data can facilitate phishing, vishing, SIM swapping, impersonation and attacks targeting customer support. The selection method declared by the attacker, however, remains to be independently verified. — Basis: wallet-KYC list; January 2026 precedents
- **[Medium confidence]** There is a physical risk for the people whose exposed data includes home addresses and indicators of crypto wealth. The risk is consistent with earlier episodes of threats and intrusion attempts associated with crypto victims, but the references to kidnapping threats and French statistics must be kept as contextual evidence, not as proof of a specific risk for every Revolut victim. — Basis: Kraken filing; Duel; franceinfo
- **[Medium confidence]** Identity documents and selfies can be reused to create synthetic identities, open accounts usable as money mules or pass KYC processes at other services. The sources on identity-mule risk highlight the combined reuse of documents and selfies, together with checks on device, address, wallet and transactional patterns. The ransom demand in Monero documents an extortion component, but on its own does not prove that the data has already been used for laundering. — Basis: nature of the data; ransom demand

- **[Medium confidence]** Secondary dissemination of the data can amplify the harm: third-party accounts can republish legible documents after the original channels are closed, while unconnected offers of Revolut accounts on onion services feed a parallel market of identities and accounts. These two phenomena must remain separate: the presence of a market does not prove that the Revolut data has already been sold or reused. — Basis: X posts of 14-15/09; onion listings.

KYC as a structural privacy risk

The case illuminates a problem broader than the single incident. The KYC framework, born to counter money laundering and terrorist financing — with obligations expanded above all after 11 September 2001 — performs a real function but, as implemented, by its nature creates centralised archives of verified identities: documents, selfies, personal data, proofs of residence, linked to wallet addresses, deposit and withdrawal histories, trading volumes. Such an archive turns the platform into a honeypot: for an attacker a KYC database is often worth more than a hot wallet, because it enables identity theft, targeted phishing, fraud and extortion. Not by chance, in the Coinbase (2025, ~69,000 users, data sold by an insider) and Revolut (2026, ~680 customers, data exfiltrated after a fraudulent request) cases, the KYC data was stolen without directly touching the funds.

The most insidious effect is that KYC links the real identity to crypto activity. Without it, a wallet address is at most a pseudonym; with KYC the exchange knows that "address X = person Y", and when that link is exfiltrated — through breach, insider or abusive request as in this case — the pseudonymity falls upstream. The same applies, in practice, to privacy coins: Monero obfuscates well on-chain, but if a user buys XMR on a KYC exchange and withdraws it to their own wallet, it is the exchange that holds the link "user → transaction → Monero address"; if that link is compromised, part of the privacy is already broken even before the blockchain.

The risk multiplies because the points of failure are not only the exchanges: identity verification is often delegated to a few specialised providers (Sumsub, Persona, Veriff, AU10TIX and the like) that manage the KYC data of dozens of platforms. An incident at a single provider exposes at one stroke the users of many operators: this is shown by the Sumsub leak, which remained undetected for months, and the exposure of AU10TIX's data protracted over time, in a landscape counting dozens of breaches affecting precisely the identity verifiers.

[High confidence on the cases; for the rest, documented debate] The criticism of KYC as implemented is not an isolated position: it is raised by digital-rights organisations (ARTICLE 19, on mandatory e-KYC as a risk to privacy and freedom of expression), security analysts, the literature on the digital euro/CBDC and the trade press. The most eloquent figure is one of scale: in 2026 the identity-verification provider IDMerit exposed about one billion records in 26 countries — confirmation, on an industrial scale, that KYC databases are dangerous targets precisely because they are built to verify identity. The recurring arguments are the excessive collection and prolonged retention of sensitive data, the opaque sharing with third parties (sanctions screening, PEP, adverse media), and the existence of alternatives — zero-knowledge proofs and non-custodial verifications — that would make it possible to ascertain identity without accumulating the archives. — Basis: ARTICLE 19; Cybernews/Zyphe (IDMerit, 2026); Cointelegraph and Bitcoin.com (Revolut case); CBDC/privacy literature.

A fundamental asymmetry emerges: users submit to continuous and increasingly invasive checks, but control over who holds those identities is comparatively weak — and the same infrastructure is the one on which regulated finance and digital-euro projects will rest. KYC, as it stands, does not eliminate the risk: it shifts a substantial part of it from the sphere of funds to that of identity and privacy, making users more exposed to fraud, extortion and targeted surveillance. The defensible direction is not to abolish it, but to reduce its surface: minimisation of the data collected, strict retention limits, reusable or decentralised verifications, and treatment of KYC archives as critical assets on a par with the funds held in custody.

In terms of incentives, KYC primarily protects the institution's compliance position; the risk, once the data is collected, falls on the user — who has no simple tools to get "cleaned" out of the databases once the data is

exposed. It is not the existence of the verification that is in question, but an implementation that retains the benefit and distributes the risk.

A clarification, so as not to force the reading: there is no causal pattern of the type “a platform introduces KYC and is therefore attacked afterwards”. The documented cases show that those hit are platforms already fully KYC — and their verification providers — precisely for the identity data they hold, regardless of when KYC was adopted (Binance in 2019, Coinbase in 2025, Revolut in 2026). Exchanges with minimal or no KYC are also attacked, but usually for the funds (hot wallets, private keys), not for personal data that largely does not exist. The risk factor is therefore not the introduction of KYC as such, but the centralised concentration of verified identities. **[Medium confidence — no evidence of a causal pattern; sample survey]**

[High confidence on the cases cited; the rest is policy analysis] — Basis: Coinbase (2025) and Revolut (2026) cases treated in the dossier; identity-verification provider breaches (Sumsub, AU10TIX); post-2001 AML/CFT framework.

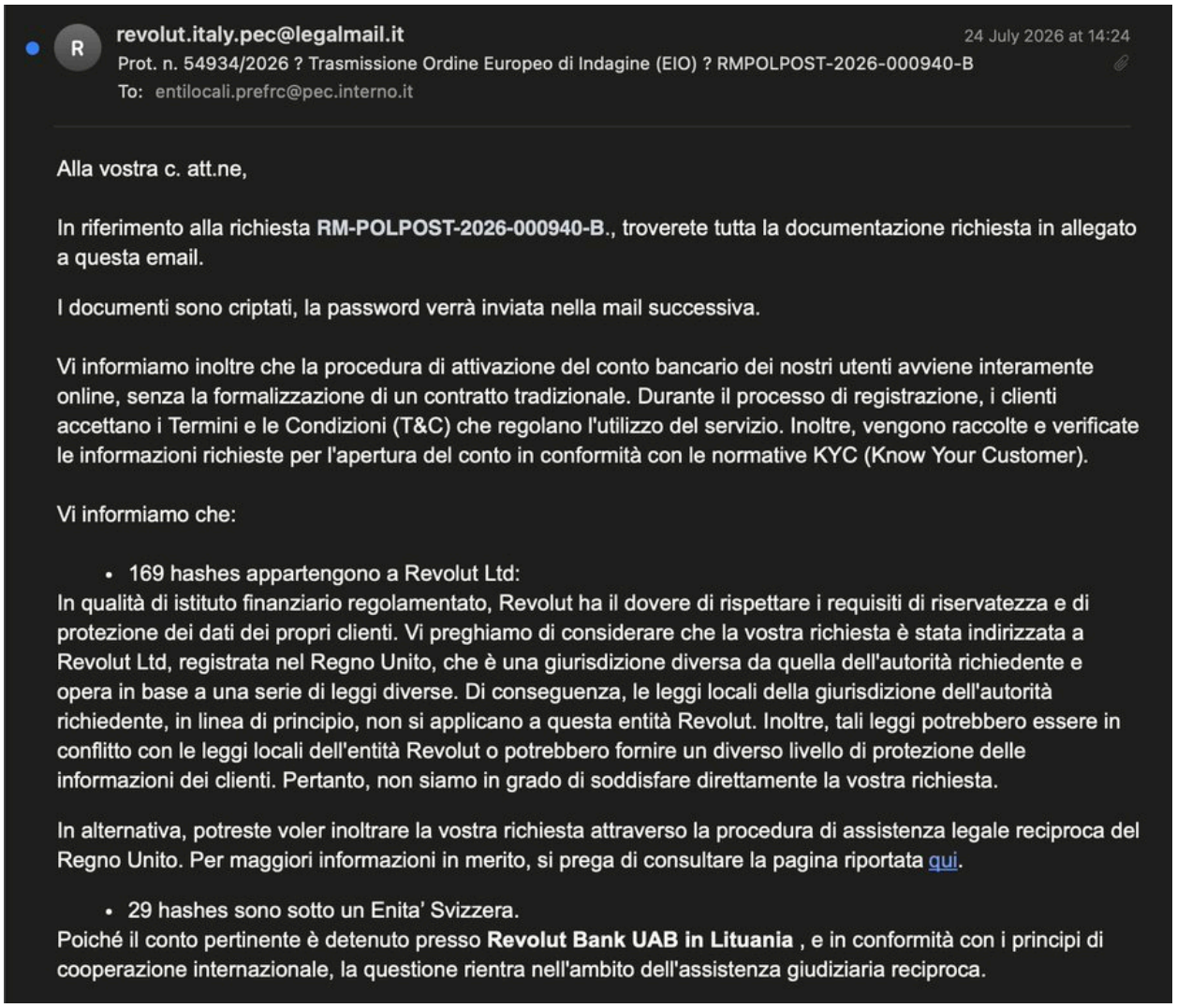
8. Missing or bypassed controls

Guiding question: which control should have prevented the delivery of the data?

Control	Status in the case	Evidence
Sender authentication	**Passed only on the technical level:** the request came from an authentic government domain/channel and, according to the available reconstructions, the email checks appeared consistent.	PEC; reconstructions on SPF/DKIM/DMARC
Independent verification of the authority	**Not evidenced:**no independent contact with the Public Prosecutor's Office or with the authority's central channels is apparent	StrettoWeb; comparison with Kraken, which verified the Irish order by contacting the court, filing para. 108
Consistency of channel and form	**Possible missed control:**an EIO sent via PEC from a prefecture office, “Postal Police” signature, Milan Public Prosecutor's Office heading and an English-language letter not consistent with Annex A	Screenshot of the EIO and the PEC
Validation of the legal basis	**Not evidenced:**absence of a judicial order in the documentation examined	StrettoWeb; Kraken filing, paras. 93 and 99–104
Jurisdiction check	**Applied but insufficient:**it filtered the recipient group company without validating the substantive authenticity of the request	PEC 24/07
Dual approval	Not known	—
Alert on mass or anomalous requests	**Not evidenced for the period prior to discovery:**the volume, repetition and structure of the requests could have constituted anomaly signals	Frame from the video; PEC; 192 messages and 33 folders, if confirmed by the documentation
Data minimisation	**Not evidenced:**selfies, account statements and transactional history potentially broader than necessary were reportedly transmitted	Revolut notice; material attributed to Duel
Handling of “corrective” responses	**Potentially counterproductive:**support reportedly indicated how to correct the request and to which company the documentation should be addressed	PEC 24/03; Duel
Tracking and audit	**Activated after the report:**the internal audit appears to postdate the discovery of the anomaly	May PEC
Protection of the institutional mailbox (authority side)	**Not publicly verifiable:**circulating credentials are reported and the mandatory application of MFA to the mailbox involved is not documented	TI source; PEC provider document
Response channel and delivery of the data (and of the key)	**Missing: according to the reconstruction, the response was sent to the same address from which the request came — controlled by the attacker —**	Reconstruction of the case; Hudson Rock (mailbox monitored by the attacker)

Control	Status in the case	Evidence
	rather than to an independent and verified channel or device; if the data had been encrypted, sending the key over the same channel would have nullified its protection.	

[Medium confidence]The speed of the response must also be read in the light of systemic pressure: the duty to cooperate with the authorities, tight deadlines and the risk of supervisory findings, sanctions or de-risking by correspondents push an institution to respond quickly and to lean towards execution — a bias the attacker exploited. This does not, however, mitigate the specific operational error: the delivery of the data (and of any encryption key) took place over the same channel as the request, i.e. towards the mailbox controlled by the attacker, instead of over an independent and verified channel or device. The defensible rule — consistent with the advisories on fake requests from the authorities (FBI, 2024) and with the controls already indicated — is twofold: verify the authority out-of-band before responding, and deliver data and keys only to an institutional endpoint obtained independently, never by “replying” to the incoming address. — Basis: reconstruction of the case; Hudson Rock; FBI PSA on fake EDR requests, 2024



revolut.italy.pec@legalmail.it 24 July 2026 at 14:24
Prot. n. 54934/2026 ? Trasmissione Ordine Europeo di Indagine (EIO) ? RMPOLPOST-2026-000940-B
To: entilocali.prefrc@pec.interno.it

Alla vostra c. att.ne,

In riferimento alla richiesta **RM-POLPOST-2026-000940-B**., troverete tutta la documentazione richiesta in allegato a questa email.

I documenti sono criptati, la password verrà inviata nella mail successiva.

Vi informiamo inoltre che la procedura di attivazione del conto bancario dei nostri utenti avviene interamente online, senza la formalizzazione di un contratto tradizionale. Durante il processo di registrazione, i clienti accettano i Termini e le Condizioni (T&C) che regolano l'utilizzo del servizio. Inoltre, vengono raccolte e verificate le informazioni richieste per l'apertura del conto in conformità con le normative KYC (Know Your Customer).

Vi informiamo che:

- 169 hashes appartengono a Revolut Ltd:

In qualità di istituto finanziario regolamentato, Revolut ha il dovere di rispettare i requisiti di riservatezza e di protezione dei dati dei propri clienti. Vi preghiamo di considerare che la vostra richiesta è stata indirizzata a Revolut Ltd, registrata nel Regno Unito, che è una giurisdizione diversa da quella dell'autorità richiedente e opera in base a una serie di leggi diverse. Di conseguenza, le leggi locali della giurisdizione dell'autorità richiedente, in linea di principio, non si applicano a questa entità Revolut. Inoltre, tali leggi potrebbero essere in conflitto con le leggi locali dell'entità Revolut o potrebbero fornire un diverso livello di protezione delle informazioni dei clienti. Pertanto, non siamo in grado di soddisfare direttamente la vostra richiesta.

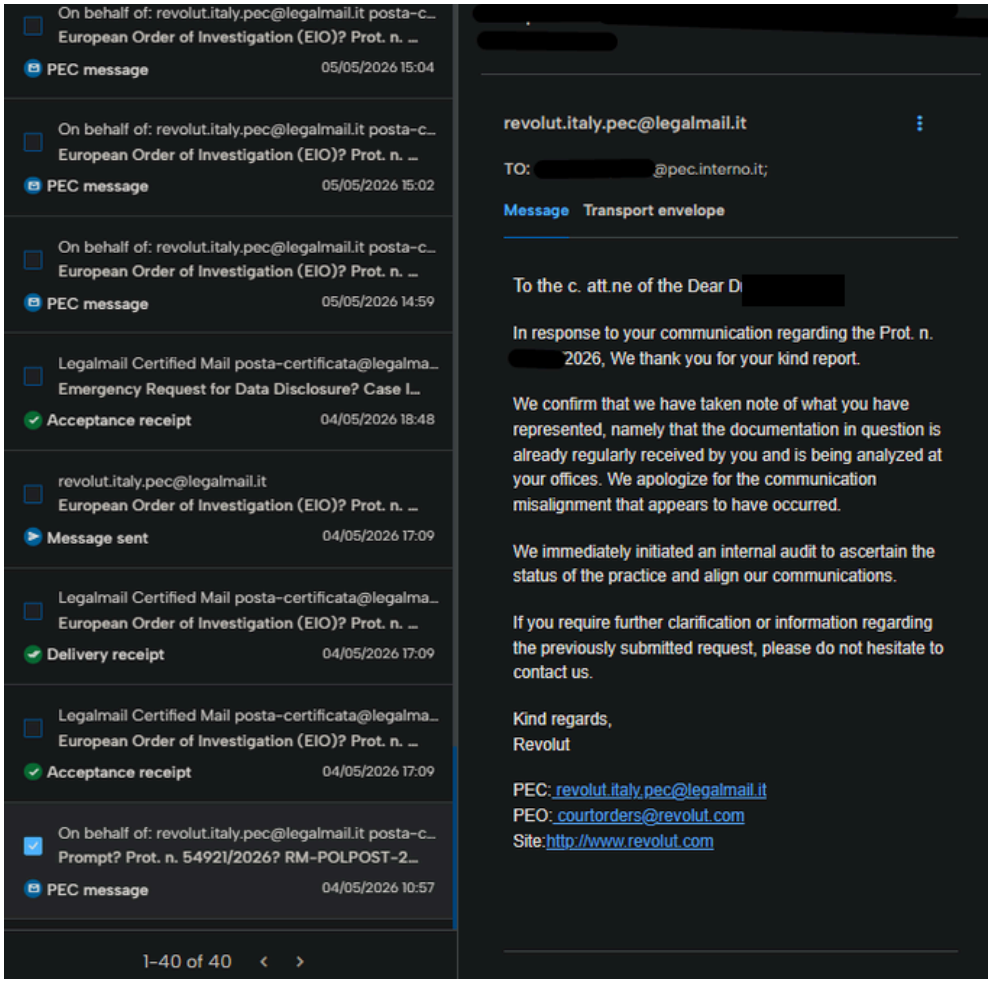
In alternativa, potreste voler inoltrare la vostra richiesta attraverso la procedura di assistenza legale reciproca del Regno Unito. Per maggiori informazioni in merito, si prega di consultare la pagina riportata qui.

- 29 hashes sono sotto un Enita' Svizzera.

Poiché il conto pertinente è detenuto presso **Revolut Bank UAB in Lituania** , e in conformità con i principi di cooperazione internazionale, la questione rientra nell'ambito dell'assistenza giudiziaria reciproca.

The documents attributed to the 24 July request show that Revolut — according to what was illustrated by Lyudmyla Kozlovska (@LyudaKozlovska on X) — applied a jurisdictional check: for 169 hashes referring to Revolut Ltd (United Kingdom) it refused direct disclosure, pointing to British mutual legal assistance; for 29 hashes, referring to a Swiss entity with an account at Revolut Bank UAB in Lithuania, it referred to mutual judicial assistance. The same communication indicates that the requested documentation was attached; from the visible part it is not possible to establish for which accounts. According to the .eml files described by Duel, the actors reportedly used transaction IDs and public wallet addresses as search keys to select

high-value crypto customers and obtain their KYC data. These elements strengthen the hypothesis of a targeted procedural abuse, but on their own do not prove that the European regulatory framework excludes a substantive verification of the requester, nor that all the data was disclosed according to the same scheme.



View of the mailbox – list of messages ("1-40 of 40"): between 4 and 5 May 2026 there appear sends, Legalmail acceptance and delivery receipts and a reply from Revolut; the subject of the exchanges "European Order of Investigation (EIO)" and "RM-POLPOST". Recipient name redacted. (screenshot received; not independently verified)

8-bis. Integration of cyber into the process of responding to requests from the authorities

The table in section 8 suggests that the main points of possible failure are organisational and procedural, not necessarily technological vulnerabilities of the banking infrastructure. In operating models where requests from the authorities are handled mainly by legal and compliance, without a structured control point for security, SOC or CTI, the trust channel can remain outside normal cyber monitoring.

What the sector's anti-fraud tools cover

- **[High confidence]** The anti-fraud and intelligence solutions adopted in the sector cover above all transactional fraud, onboarding, compromised credentials and cards, as well as movements between traditional accounts and on-chain activity. The Nasdaq Verafin–Q6 Cyber, Nasdaq Verafin–Alloy and Nasdaq Verafin–Stablecore partnerships are examples of this direction: dark-web intelligence, identity-risk signals, consortium data and correlation between traditional and digital financial activity — Basis: Nasdaq Verafin press releases

These tools can be useful downstream, to detect the fraudulent use of KYC data stolen at other institutions, but they are not necessarily designed as control systems for data requests coming from public authorities. A disclosure request is not a financial transaction and may therefore not generate the same behavioural alerts.

[High confidenceon the convention] Convention of the Prefectures' PEC addresses. The offices' addresses follow a uniform scheme of the type <office>.pref<province code>@pec.interno.it, as shown by the lists published by the individual Prefectures (example: Prefecture of Cosenza, snapshot of 22/12/2025, which reports entilocali.prefcs@pec.interno.it for Area II – Liaison with Local Authorities). The predictability of the scheme means that the formal consistency of the sender address does not constitute a verification element: a plausible address can be derived without any access to the systems. — Basis: public lists of the Prefectures (Internet Archive)

[High confidence on the IPA data] Digital domicile and IndicePA. The digital domicile of the Prefecture of Reggio Calabria registered in IPA is protocollo.prefrc@pec.interno.it, registered since 12/04/2019. The address used for the requests to Revolut (entilocali.prefrc@pec.interno.it) is not registered in IPA, which, however, records the digital domiciles of entities and their branches and not every internal mailbox: its absence therefore does not prove that the mailbox did not exist. From this follows a minimum check applicable by any recipient: verify that the sender address corresponds to the digital domicile published in IPA for the indicated entity and, in case of discrepancy, ask the entity for confirmation on an independent contact. — Basis: IndicePA

[High confidenceon the provider] PEC provider. The pec.interno.it domain is hosted on InfoCert Legalmail (MX record mx.cert.legalmail.it). Revolut's PEC (revolut.italy.pec@legalmail.it) is also on Legalmail/InfoCert: the sender and recipient of the exchanges are therefore on the same provider, which makes the environment shown in the screenshots consistent (a @pec.interno.it mailbox opened in the InfoCert webmail). The consistency of the environment does not, however, amount to the authenticity of the individual screenshots, which remain material circulated by the actor. — Basis: DNS MX record of pec.interno.it

[High confidence on how PEC works] Manning of the mailbox and traffic traces. Prolonged use of an institutional PEC mailbox entails traffic visible in the mailbox itself: acceptance and delivery receipts for every send, replies and reminders from the recipient, sizeable attachments that affect the available quota, provider notifications. The failure to detect it for several months implies one of these conditions: absence of monitoring of the mailbox, systematic deletion of the messages by whoever controlled it, or failure to report by whoever saw the traffic. The message log retained by the PEC provider for thirty months nonetheless allows the reconstruction of senders, recipients, dates and identifiers, regardless of the deletions carried out on the mailbox. — Basis: certified-email (PEC) rules

Minimum controls on requests from the authorities

Control	Who	Description
Out-of-band verification	legal / compliance	contact with the authority through official contacts obtained independently, never those present in the request
Formal consistency	legal	office competent by subject matter, signature, addressee authority, prescribed channel (EIO via the national executing authority)
Legal basis	legal	judicial order, case number, identifiable magistrate
Dual approval and minimisation	legal + security	mandatory for requests with KYC or biometric data or referring to multiple customers
Volume and frequency thresholds	security / SOC	alerts per sender on the number of requests, number of customers, lists of hashes or wallets
Response to refusals	compliance	no corrective guidance to an unverified requester

Escalation triggers for high-risk institutional requests

The following table introduces a technical-organisational decision gate for the Law Enforcement Response process: the triggers do not generically classify the risk, but indicate when to halt automatic disclosure and which owner must activate the reinforced control.

Activation signal	Observable condition	Required control / owner
Anomalous EIO or cross-border request	EIO or cross-border request received directly, or coming from a non-competent office or from a channel not consistent with the proceeding.	Out-of-band legal validation with the competent authority and temporary block on disclosure.
Documentary inconsistency	Signature, heading, language, indicated authority, case number or attachments not consistent.	Legal review, verification of the legal basis and preservation of message, attachments and metadata.
High-impact disclosure	Request for KYC, biometric, transactional, crypto data or referring to multiple customers.	“Four-eyes” approval by Legal/Compliance/Security and a data-minimisation gate before delivery.
Adaptive requester	Reformulations after a refusal, progressive corrections, anomalous urgency or requests for alternative contacts.	Compliance review with SOC/CTI escalation and limitation of the operational guidance provided to the requester.
Compromised-channel signal	Mailbox, domain or infrastructure associated with exposed credentials, anomalous access, known abuse or inconsistent behaviour.	SOC/CTI triage, verification with the entity that owns the channel and raising of the risk level.

Operational rule:the presence of a high-impact trigger, or the combination of several triggers, must suspend automatic disclosure until the reinforced controls are completed and a documented decision is taken by the owners involved.

The role of cyber and CTI

Cyber and Cyber Threat Intelligence (CTI) should intervene before the disclosure of the data, not only after a possible abuse. Their task is to verify the technical and behavioural context of the request, raise the risk level when convergent signals emerge, and provide independent elements to legal, compliance and investigations.

Message analysis

The verification should include:

- full headers, Message-ID, SMTP path and timestamps;
- domain authentication, including SPF, DKIM and DMARC;
- history of the sender mailbox and domain;
- age, competence and behaviour of the mailbox;
- any anomalies in the signature, attachments or contacts;
- use of a new mailbox, not consistent with the declared office or not competent by subject matter.

The technical analysis does not on its own prove the legitimacy of the request, but it can highlight spoofing, compromise, anomalous forwarding or deviations from the normal process.

Note: in the report on malicious campaigns of 2025 (published on 10/02/2026), CERT-AGID indicated that PEC campaigns exploited above all compromised legitimate mailboxes, in addition to addresses registered ad hoc and then decommissioned following a report to the providers. On 15/06/2026 it announced that, since January 2026, it had handled over 650 events relating to PEC mailboxes abused or registered for illicit purposes, asking providers to reset compromised mailboxes and decommission those created for malicious purposes. — Basis: CERT-AGID, 2025 report; CERT-AGID, notice of 15/06/2026

Threat intelligence on mailboxes

CTI can monitor, in compliance with the legal basis and internal rules, infostealer logs, combolists, forums and other criminal spaces to identify credentials or references attributable to entities and authorities. A match does not prove the compromise of the mailbox: it may reflect old, reused, falsified data or data referring to a third-party service. However, it should raise the risk level and trigger an independent check; the initial findings of the Postal Police, reported by the press on 18/09, do not confirm the theft with the entity that owns the mailbox.

Pattern detection

It is useful to automatically correlate:

- lists of hashes or wallets used as the sole search key;
- requests for re-addressing or “correction” after a refusal;
- urgency, threats and anomalous deadlines;
- requests to send to alternative addresses;
- serial requests or a sudden increase in the customers involved;
- encrypted attachments and passwords transmitted over separate channels;
- repetition of subjects, references, hashes, wallets or document templates.

The correlation should not produce an automatic refusal based on a single indicator. It should instead generate a risk assessment, a preservation of the artefacts and, when necessary, an escalation to security, legal and compliance.

Sharing of indicators

Verified indicators can be shared with CERTFin, CERT-AGID, ACN and with the entity that owns the suspect mailbox, using the appropriate channels and applying minimisation, access control and traceability. CERTFin presents itself as the CERT of the Italian financial sector and operates in support of the prevention and management of cyber threats in the financial sector. The sharing should clearly distinguish between observed data, verified data, analytical hypothesis, confidence level and action required of the recipient.

Joint exercises

Legal–compliance–security simulations on scenarios of impersonation of the authorities are advisable, including the Kraken and Revolut cases as test scenarios. The exercise should verify:

- who receives and records the request;
- who assesses authenticity, competence and legal basis;
- who decides on the suspension of disclosure;
- how the authority is contacted through an independent channel;
- what evidence is preserved;
- when and how external reporting is carried out.

Obligations and good practices

- **[High confidence]** General obligation. The GDPR requires a legal basis for the processing and communication of data, as well as security measures adequate and proportionate to the risk. The text of the regulation links security to the assessment of risks and to measures suitable to protect confidentiality, integrity and availability. — Basis: GDPR; DORA. Financial scope. DORA applies from 17 January 2025 to financial entities within its perimeter and governs, among other things, ICT risk management, incidents, operational resilience and related governance.
- **[Medium confidence]** Good practice, not necessarily a specific obligation. There is no evidence, on the basis of the sources cited, of a general and detailed obligation imposing on every institution a single procedure to verify the substantive authenticity of requests from the authorities. This does not mean that verification is optional: it means that its concrete configuration derives from the set of obligations on legal basis, security, governance, risk management and data protection. — Basis: cited legislation; statements by Kozlovska and Kodex

The limit is not necessarily the absence of anti-fraud technology, but the organisational separation between those who receive the requests, those who assess their legitimacy and those who monitor the signals of compromise. Security should enter the process before the disclosure of the data, not only after the data has been used for fraud.

9. Indicators of compromise

9.1 Technical indicators

Indicator	Type	Status
entilocali.prefrc@pec.interno.it	PEC email address presumably abused	Reported by third parties; authenticity and control of the mailbox not verified
Subjects: “Trasmissione Ordine Europeo di Indagine (EIO)” and “Emergency Request for Data Disclosure”; references RM-POLPOST-2026-000940-B, Prot. no. 54921/2026 and 54934/2026	Request pattern	Reported by third parties
Heading “Public Prosecutor's Office at the Court of Milan”, Via Freguglia 1, English language and absence of signature	Potentially forged document	Reported by third parties, documentary indicator.
imnotavillain[.]xyz — registered 14/09/2026 (NICENIC INTERNATIONAL GROUP CO., LIMITED; nameservers ns3.my-ndns.com / ns4.my-ndns.com)	Domain associated with the actor	Confirmed via WHOIS.
iamnotavillain[.]com — registrar Tucows Domains Inc.; Njalla nameservers; registered on 15/09/2026 and updated on 16/09/2026.	Domain associated with the actor	Confirmed via WHOIS, if verified against the original record
revoloot[.]lol - registrar NameSilo, LLC dnsowl.com	Extortion site associated with “Revolut Smilik”	Reported by the Telegram channel. Server hold and client hold indicate a status of suspension or block at the registry/registrar
@revolutsmilik, t.me/backupsmile1231	Communication channels	Backup channel
Session ID (Revolut Smilik) 05a6f11c1dd5897925a29c9b02966d99f62401b0fc6282b3b4f13e59a3bcad805f	Contact identifier	Confirmed in the messages as a contextual indicator;
Session ID (IAmNotAVillain) 0548b3c2be496218baa2314386787badfd458a868240a19ede82eabb6a13dd2c26	Group contact identifier	CONTACT tab of the group's site (“Same place for staff, press, and users”). Session ID = public key of a decentralised messenger. Usable as an identifier/IoC.
Wallet XMR 8BvXFt6v7aSR3Qs9SPgBVLWQzAragHtTiXn3Us3Eh2wLjED1zE4D7a5KxsRE3Wn4e1CjjLJydavscdcwge2UurTUKsgGBXe	Monero (XMR) ransom wallet	Full address from the extortion site. Monero conceals amounts and counterparties: payment, balance and flows are not verifiable on the blockchain by an external observer (cf. note on the limits of traceability). Usable only as an identifier/IoC
ibb[.]co/gBcT44h	Image-hosting URL containing a wallet–KYC list	Confirmed as a link shared in a Telegram message; content, provenance and authenticity to be verified

Note — The Monero ransom and the limits of traceability

The ransom XMR address (8BvXFt6v7aSR3Qs9…UurTUKsgGBXe) cannot be queried on an explorer like a Bitcoin or Ethereum address. Monero conceals by design three elements of on-chain transactions: the amounts (RingCT), the sender (ring signatures) and the recipient (stealth address). Direct analysis on the blockchain is therefore much weaker than on Bitcoin: one does not follow a flow "address A → B → C".

Monero is not, however, "perfectly untraceable". View keys, if voluntarily shared or seized, allow all incoming and outgoing transactions of a wallet to be seen; temporal-correlation techniques, network analysis and clustering can provide clues, especially when combined with data external to the blockchain.

It is precisely off-chain that anonymity tends to break. Real investigations into Monero typically rely on exchange KYC (when XMR enters or leaves a regulated platform, the exchange knows the user and, on a warrant, hands over the logs), on forensics on seized devices (extraction of private or view keys from wallets and memory), on network metadata and undercover operations, and on users' operational errors (identity reuse, IP leaks, view keys carelessly shared).

Research on tracing Monero has a history, and it is a continuous chase. As early as 2017 the Bitcoin ransom of WannaCry was converted into Monero through an exchange service, and the useful trail was not the blockchain but the service's logs; in 2021 those transactions were the subject of a public forensic analysis. Between 2024 and 2025 sector reviews (TRM Labs) and academic research dedicated to Monero wallet forensics showed two converging things: some on-chain heuristics exist but their effectiveness declines as the protocol is hardened — mandatory increases in ring size, rapid fixes of flaws — while genuinely effective tracing goes through off-chain artefacts, i.e. wallets and devices. The 2026 operations confirm the picture.

Some cases show it. In Norway, in 2026, Kripos used a new method of tracing Monero in an international operation on dark-web forums that ended with 28 arrests in several countries — not by "reading the blockchain", but by combining the tracing of XMR with traditional investigations and international cooperation. In the Vastaamo case, in Finland, the police stated they had "traced" a Monero payment, but the attribution came about through other elements (exchange data, seizures, the Bitcoin part of the operation); the claim of a purely on-chain tracing is contested by experts.

For the case under examination it follows that, for an external observer (press, users, competitors), it is practically impossible to verify whether the ransom was paid: the choice of Monero makes the payment unverifiable on the blockchain. Only the authorities, with access to the exchanges, the seized wallets or the view keys, could in perspective reconstruct the flows. The indirect routes already known remain: checking whether the address is flagged (Chainabuse, threat-intelligence feeds), which would link the campaign to others, or a possible transaction key published by whoever pays.

Direct verification (20/09/2026). The address cannot be queried on a public block explorer and its decoding confirms its nature as a mainnet subaddress; the view and spend keys that some explorers show are the public ones, derivable from the address itself, and allow neither viewing nor moving funds. Verifying the actual receipts would require the wallet's private view key, which is not public: a check attempted with the public key alone produces no valid matches and has no evidential value. The address, moreover, is not flagged on Chainabuse nor present in indexed public sources: no known public footprint as of the date. **[High confidence — direct verification]**

[High confidenceon how Monero works; medium on the operational limits of tracing] — Basis: characteristics of the Monero protocol; TRM Labs (2024 review); Forensic Science International: Digital Investigation (wallet forensics, 2025); CyberScoop/Neutrino (WannaCry, 2017) and analysis by N. Bax (2021); Euronews, TechNadu (Norway, Kripos 2026); BleepingComputer (Vastaamo case).

9.2 Behavioural indicators for an institution

The following signals may indicate fraudulent requests, impersonation of authorities or attempts to evade normal legal controls. No single indicator is conclusive: the assessment should be based on the combination of signals, on the independent verification of the requesting authority and on the consistency of the proceeding

- Requests coming from institutional domains, but from mailboxes or offices not competent by subject matter.
- Inconsistency between the sending office, the signature, the addressee authority and the declared proceeding.
- European Investigation Orders or requests for judicial assistance received directly, instead of through the channel of the competent executing authority.
- Extensive lists of transaction hashes or wallet addresses used as the sole search key, without further identifying elements or evidential context.
- Absence of an order, a verifiable case number or a reference to an identifiable magistrate.
- Repeated requests from the same sender, with increasing volume or an ever-larger number of customers involved.
- Requests for "correction" or re-addressing after a formal refusal or a request for additional information.
- Language of urgency, threats, anomalous deadlines or a request to send to an alternative address.
- Encrypted attachments with a password transmitted over a separate channel, especially when the volume of data requested is high.
- Requests addressed to multiple group companies without a clear jurisdictional justification or a delimitation of the perimeter.
- Repetition of the same references, subjects, hashes or wallets in successive messages, even after negative responses or requests for clarification.

Escalation criterion

The simultaneous presence of several signals should trigger a reinforced verification before any disclosure of data. In particular, the institution should suspend operational compliance when the request presents inconsistencies between authority, competence, proceeding and transmission channel, or when the sender attempts to replace the normal procedure with urgency, pressure or alternative contacts.

The verification should include at least:

- authentication of the sender through an independent and already-known channel;
- checking of the authority, the office and the proceeding in the appropriate registers or institutional contacts;
- examination of the integrity of the attachments and the technical headers;
- confirmation of the legal basis, the subjective and temporal scope and the data actually requested;
- recording of the request, the outcomes of the checks and any anomalies.

The indicators constitute risk signals and do not, on their own, prove either the falsity of the request or the compromise of the institutional identity.

10. "Lessons learned" for a banking institution

- **[High confidence]** An authentic institutional domain does not, on its own, prove the substantive authenticity of the request. PEC too certifies the sending and delivery of the message, but does not

prove that the person controlling the mailbox is the party authorised to formulate that request. — Basis: Kraken and Revolut cases; Kodex statement

- **[High confidence]** A formal refusal that explains in detail how to correct the heading, jurisdiction, format or procedural references can provide the attacker with a guide to passing the next check. This does not mean eliminating the reasons for refusals. It means adopting a controlled response. — Basis: PEC 24/03 and 24/07; Kraken filing
- **[Medium confidence]** The scheme is plausibly transferable to Italian institutions because the authorities and many organisations use PEC for formally relevant communications. However, it should not be presented as proof that every bank receives or handles requests with identical procedures. The contextual figure is significant: on 15/06/2026 CERT-AGID announced that, since January 2026, it had handled over 650 events relating to PEC mailboxes abused or registered for illicit purposes, asking providers to reset compromised mailboxes and decommission those created for malicious purposes. — Basis: CERT-AGID, 2025 report; CERT-AGID, notice of 15/06/2026
- **[Medium confidence]** Investments in anti-fraud on transactions, onboarding and on-chain activity may not cover the process of responding to requests from the authorities. The risk arises in the border zone between compliance, the legal office and information security. — Basis: Nasdaq Verafin press releases August-September 2026. Nasdaq Verafin's recent initiatives show a growing integration between risk signals, identity and fraud prevention along the customer lifecycle; this does not, however, prove that the problem of fraudulent requests to the authorities is automatically covered by such tools. The operational lesson is to establish a cross-cutting control before disclosure, with shared escalation criteria and clearly assigned responsibilities.
- **[Medium confidence]** After the incident, the damage does not remain limited to the database or the internal process. It can extend to: secondary dissemination of the data, media and political use of the case, regulatory pressure and loss of trust in institutional channels. — Basis: sections 7 and 13

11. Confidence assessment

Assessment	Confidence	Main gaps
Abuse of the process of responding to the authorities, not an intrusion into Revolut's systems	High	The exact nature of the access and of the operational flow remains to be fully documented
Use of a legitimate Italian government domain	High	A complete public confirmation from the Ministry of the Interior is missing; it remains to be established whether the mailbox was compromised or cloned; on the specific case
Mailbox referring to the Local Authorities Office of the Prefecture of Reggio Calabria	Medium	Attribution based on screenshots and press; no official public confirmation from the entity
About 680 customers selected through blockchain analysis	Low	Number and method are attributed to the attacker or reported by the press; not confirmed by Revolut
Requests protracted for several months, with the precise duration not confirmed	Medium	Sources diverge on the precise duration and on the start date; use “for several months” pending precise documentary confirmation
Scheme analogous to the 2025 Kraken case	High	The analogy concerns the abuse of requests apparently coming from authorities; it does not imply identity of the actors
Same actor as the Kraken 2025 case	Low	No independent technical or evidential link
Access to law-enforcement systems and exfiltration of 147 GB	Low	Attacker's claim and a screenshot of a folder, without independent verification. The initial findings of the Postal Police, reported by the press on 18/09, do not confirm the exfiltration of the 147 GB.
Attack capability	Medium	The actor demonstrated at least moderate capability for procedural abuse and social engineering, exploiting institutional channels, knowledge of the response flows and targeted selection of victims. The available evidence is not, however, sufficient to attribute an advanced technical capability or a sophisticated compromise of the systems.
Ransom of 3 million dollars in XMR	Medium	The demand for 6,000 XMR is reported by the press; it is not confirmed as a demand received directly by Revolut
Risk replicable towards Italian banks	Medium	In the material examined there are no independent cases in which an Italian bank has already suffered the same scheme

11-bis. Open questions

Was the mailbox entilocali.prefrc@pec.interno.it active before 2026? When was it created and at the request of which account?

Is it still active, or has it been decommissioned, and on what date?

What do the logs retained by the PEC provider — for at least thirty months under Art. 11(2) of Presidential Decree 68/2005 — show about the traffic of the months concerned?

Was the point of entry the theft of credentials, an abuse of administrative privileges, or an activation by procedural means?

When did the administration become aware of the anomalous use of the mailbox?

To which address were the requests to Revolut actually delivered, and how were they routed between the Italian branch and the Lithuanian entity?

What does the original text of the communication in which Revolut asks for the destruction of the documentation already sent say, and at what stage was it sent?

Are the Swiss account documents present in the published material compatible with the jurisdictional refusal declared on 24/07, or do they come from an earlier request actually executed?

Note: these are elements that depend on internal records and on investigative acts covered by investigative secrecy. Their absence from this document is not to be read as excluding any hypothesis.

12. Recommendations

Immediate

- Make out-of-band verification mandatory for every data request from an authority: contact the competent office through official contacts obtained independently, never through the contacts present in the request.
- Check the consistency between sender, signature, addressee authority, legal basis, subject, data perimeter and prescribed channel.
- For an EIO, verify the issuing authority, the executing authority, the form, the language, the proceeding and transmission through the appropriate channel. The EIO is based on mutual recognition and follows a standardised template
- Pre-emptively block requests that use lists of hashes or wallets as the sole search key, that concern many customers, or that request KYC, identity documents or biometric data.
- Apply a reinforced block when the request comes from a new mailbox, from a non-competent office or from a sender already associated with anomalous requests.
- Launch a retrospective review of the requests executed in the last 18 months, starting with those received from mailboxes not competent by subject matter, with high volume or with repeated indicators.

Process

- Require dual approval from legal and security for mass, cross-border requests or those containing KYC, biometric or financial data.
- Apply minimisation: disclose only the data necessary, for the period and purpose indicated in the proceeding.
- Define volume and frequency thresholds per sender, domain, office and customer; generate automatic alerts when the thresholds are exceeded.
- Create a centralised and immutable register of requests, with sender, timestamp, verification carried out, legal basis, data disclosed, approvals and outcome.
- Use standard responses to refusals, without explaining to an unverified requester which internal checks must be passed or how to correct the request.

- Set up a separate path for emergencies, with mandatory call-back, documented approval and subsequent review.
- Retain the original message, headers, attachments, logs, decisions and verification communications to allow audits and forensic analysis.

Ecosystem

- Share verified indicators with CERTFin, CERT-AGID and ACN, according to the applicable channels and with adequate data minimisation. CERTFin promotes the timely sharing of information on threats, vulnerabilities, incidents and lessons learned in the financial sector.
- Report suspicious institutional mailboxes to the entity that owns them and to the competent PEC provider, distinguishing between abuse of the mailbox, spoofing and compromise not yet proven.
- Assess the use of secure judicial channels and verified exchange tools. eEDES supports the digital exchange of EIOs and requests for judicial assistance between competent authorities
- Train compliance, legal, law-enforcement response and security on the impersonation of the authorities.
- Run exercises with scenarios based on the Kraken and Revolut cases, including a compromised PEC, an urgent request, a wallet list, a formal refusal and an attempt at re-addressing.
- Monitor mentions of the institution and customer data on Telegram, forums and extortion sites, with procedures to preserve the evidence without interacting with the actors.
- Prepare a communication plan for the customers involved, including phishing, extortion, doxxing and, where appropriate, physical risks.

No request should be considered automatically authentic merely because it comes from an institutional mailbox or domain. The institution must, however, comply with the applicable response deadlines through an accelerated authentication path: out-of-band verification, checking of the proceeding, confirmation of competence and an interlocutory or reasoned response when disclosure cannot yet be carried out.

13. Geopolitical and regulatory context

The case can be placed within a broader debate on trust in institutional channels, on the coercive use of financial systems and on the security of judicial-cooperation mechanisms. It is necessary, however, to distinguish the actual text of the rules and resolutions from the political interpretations developed on the basis of the Revolut case.

Transnational financial repression

- **[High confidence]** The Hague Declaration of the OSCE Parliamentary Assembly includes a resolution on transnational financial repression and on the instrumental use of AML/CFT tools, judicial cooperation, INTERPOL and cyber legislation. The text concerns above all the abuse of authentic tools by foreign States to surveil, intimidate or exercise economic coercion beyond their own borders. Basis: Kozlovska's posts on X; text of the resolution. The OSCE PA resolution does not appear to directly govern the falsification or theft of an institutional mailbox of an EU State. The link with Revolut is analogical and political, not a textual consequence of the resolution.
- **[Medium confidence]**Kozlovska's thread of 17 September 2026 specifies the mechanism: alongside spyware — the subject that same day of a joint NCSC-FBI-AIVD alert on Iranian tools against dissidents and journalists — there operate quieter and often more effective channels, all “under the cover of legitimate international cooperation”: judicial assistance (MLAT), INTERPOL notices (Red, Diffusion and the more recent Silver and Purple), AML/CFT requests on a FATF basis, and civil, arbitration or criminal proceedings opened on European soil. The thesis is that, with the stacking of digital identity, age verification and proposals such as “Chat Control”, the same inter-state requests that today freeze an

account will tomorrow be able to revoke access to a service: “States like Iran will not need to hack anyone; they will ask an EU counterpart to flag a target's digital identity”.

- **[Medium confidence]**The nexus with the case is architectural, not one of actor. The KYC model makes every user an “identified node” — a verified identity linked to accounts, cards, wallets and transaction history — placed in compliance databases exposed to requests from national and foreign authorities. The same “trusted channel” that in this case was abused with a fraudulent request of criminal origin can, from the perspective of transnational financial repression, be activated by a State with formally legitimate requests, without any “hack”. The distinction must, however, be kept firm: nothing links the Revolut incident to a state operation — the actor is criminal and the motive remains open. What the two planes share is the vulnerability of the trusted architecture, not the subject who exploits it. The European Parliament (recommendation of 16 June 2026) and the OSCE Parliamentary Assembly (The Hague, July 2026) have called for measures precisely in this area.
- **[High confidence**on the documents; medium on the architectural nexus, which is analytical] — Basis: L. Kozlovska (X, 17/09/2026); joint NCSC-FBI-AIVD alert (September 2026); European Parliament, recommendation on transnational repression (16/06/2026); OSCE PA, The Hague (July 2026).

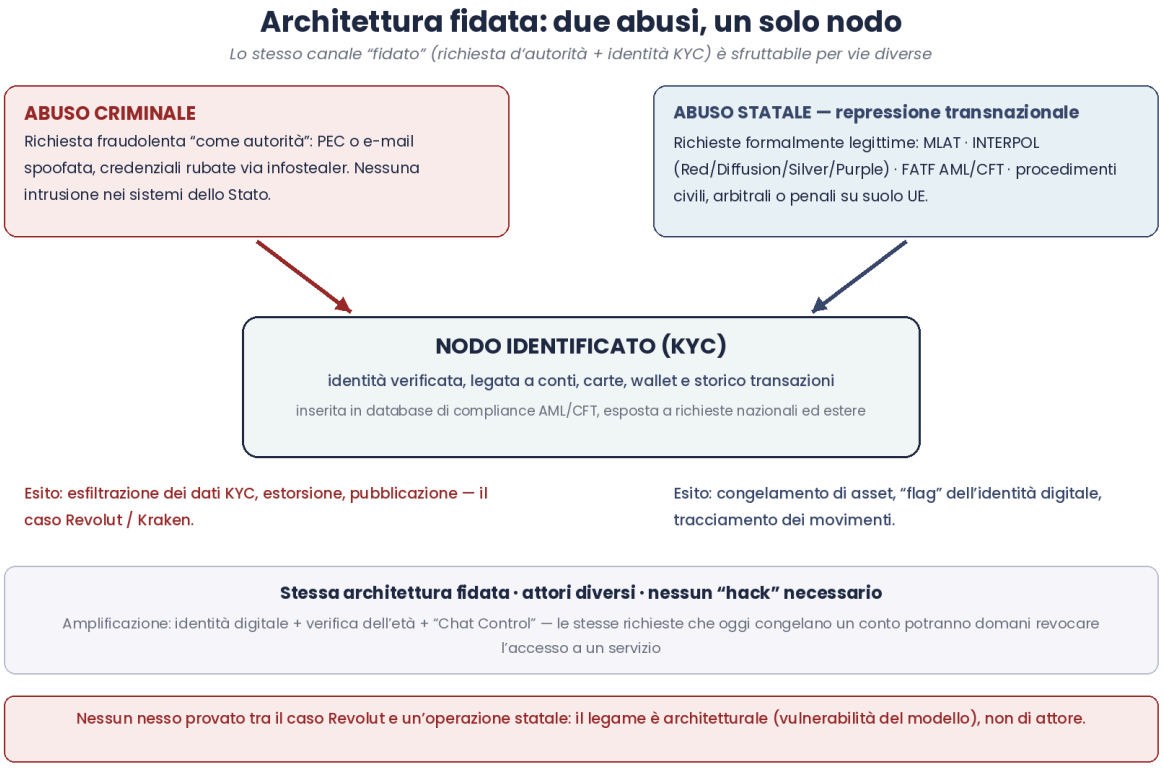


Figure — The trusted architecture and its two abuses: the same identified node (KYC) is reachable by a fraudulent criminal request or by a formally legitimate inter-state request. The link between the two planes is one of method, not of actor.

Responsibility of the company and of the rules

- **[Medium confidence]** The debate is divided between a reading that attributes the main responsibility to the company, for having carried out insufficient checks on the substantive authenticity of the requests, and a reading that highlights the limits of the regulatory framework, characterised by obligations of rapid cooperation, the absence of a single and detailed procedure to verify each request, and the growing concentration of data through mechanisms such as DAC8. The two interpretations are not mutually exclusive: an institution may be required to respond within short deadlines and, at the same time, have to adopt independent controls to avoid disclosing data to an unauthorised party. The statements of the customer involved, of Duel and of Lyudmyla Kozlovska, together with the French litigation on DAC8, support the existence of the debate, but on their own do not allow the definitive

legal liability of Revolut or the illegitimacy of the regulatory regime to be determined. — Basis: statements of a customer involved, of Duel and of Kozlovska; French Council of State on DAC8

- **[Medium confidence]** From this comes a reading that the dossier shares: in this case what was "breached" was not a Revolut system — there was no intrusion or theft of funds — but the system. The flaw exploited is structural: the channel through which an institution is required to act on a request apparently coming from an authority, and the model that concentrates verified identities in centralised archives. Any operator following the same rules is exposed to the same vector; Revolut is the instance in which the problem emerged, and its verification shortcomings — requests executed for months without adequate controls — aggravated it, but are not its root. In this perspective there is a foundation to the alarm, supported among others by Lyudmyla Kozlovska (Open Dialogue Foundation), that the mechanisms of financial surveillance and identity verification, born against money laundering and terrorism, can be diverted and turned into instruments of abuse and of risk for the very people they should protect. — Basis: dossier analysis; L. Kozlovska / Open Dialogue Foundation ("hijacking financial surveillance").

DAC8 and data concentration

- **[Medium confidence]** The French litigation brought by Bull Bitcoin and Paymium concerns the national decree implementing DAC8 (décret 2025-1276) and the obligations to collect and transmit tax data on users of crypto-assets. On 14 September 2026 the Conseil d'État rejected the application for urgent suspension (référé-suspension, no. 519158), holding that the mere possibility of a data-breach risk, of very low probability, does not constitute urgency; the judgment on the merits remains pending. The Revolut case can be used as a political argument on the risk of concentration and transfer of data, but it does not prove that DAC8 caused the incident, nor that the DAC8 regime is the legal channel used to obtain the data. The connection is one of policy and data governance, not of technical causality. — Basis: bitcoin.fr; Conseil d'État decision no. 519158.

France and physical risk

- **[Medium confidence]** France, among the countries most affected by the criminal risks linked to the crypto sector and the home of Revolut's new banking licence since 10 August 2026, constitutes a relevant context for understanding the geopolitical and regulatory dimension of the case. The theme connects both to the wave of kidnappings and extortion activities directed at operators and subjects involved in crypto-assets, and to the litigation brought by Paymium and Bull Bitcoin against the French implementation of DAC8. The link is, however, contextual and does not prove that the Revolut case was caused by DAC8, nor that the incident is directly connected to the kidnappings that occurred in France. — Basis: franceinfo; PNACO; Cointelegraph

e-Evidence and eEDES

- **[Medium confidence]** The decentralised IT system provided for by Regulation (EU) 2023/1543 links the competent authorities to service providers for European production and preservation orders. The exchange between judicial authorities for EIOs and judicial assistance is instead entrusted to eEDES, whose reference implementation portal is still in preparation on the e-Justice portal. — Basis: EUR-Lex; Eurojust; e-Justice portal — Basis: European Commission; EUR-Lex

Reputational dimension and listing

The case falls at a time when Revolut is preparing a possible listing. According to the press (Economy Magazine, 18/09/2026), the founder Nik Storonsky is considering a dual listing in London and on the Nasdaq, with a horizon indicated at 2028 and subject to market conditions; after a secondary sale of shares in July 2026 the private valuation is estimated at around 115 billion dollars, with the Financial Times indicating up to 200 billion as a possible IPO valuation. The same source reports that of the roughly 680 customers involved only 8 would be Italian, most in France, Switzerland and other European countries.

To this is added a delicate and current regulatory step: in September 2026 Revolut obtained the OCC's conditional approval for a US national bank charter (the Fed and FDIC remain to be cleared) and is in the operational phase of that charter. According to the analyst Jason Mikula it is this — more than the listing, which Storonsky himself places no earlier than 2028 — that is the "sensitive moment" in which the incident falls; the company's valuation is estimated at around 110 billion dollars. [High confidence on the regulatory and financial data; nexus with the incident not demonstrated] — Basis: Bloomberg (03/09/2026), OCC Corporate Decision #1390, PYMNTS; Jason Mikula (20/09/2026).

Hypothesis — motive (open). The motive cannot be determined and must not be closed. The ransom demand in Monero indicates an economic component, but does not exhaust the question: the choice to operate through a real Italian government mailbox is deliberate and strategic. In Italy PEC has legal value and enjoys a high level of institutional trust; hooking the operation to that channel confers far greater credibility and impact than an ordinary request, and it is what made the request "seem true" in the eyes of those who had to execute it. Maximising credibility and impact in this way is compatible both with an economic aim (public embarrassment forces payment) and with an aim of reputational or systemic damage, all the more so in a pre-listing phase. The available elements do not allow one to favour either: both must be kept open. Reputational damage remains, in any case, a real effect, regardless of intent.

[Medium confidence] The very form of the extortion reinforces the openness of the motive. A purely economic demand normally goes through a direct and confidential channel with the victim; here the ransom demand (3 million dollars, ~6,000 XMR) was made publicly — on the group's site, on Telegram and through the press — while Revolut states it received no direct contact and did not negotiate, and no payment is apparent. A public demand without a direct channel reduces the probability of collection but maximises reputational damage, and it is accompanied by the explicit rhetoric of the intermediary (Duel), which declares it wants to make public "every element" to show "Revolut's failure" and "the stupidity of the way KYC is conducted today". It is a profile compatible with a mixed motive — economic but also reputational and ideological — more than with a "clean" extortion. This does not imply external direction nor a causal nexus between the adoption of KYC and the attack: the selection of data-rich, high-visibility targets is an effect of opportunity (honeypot), not proof of orchestration. — Basis: Reuters (16/09/2026); Revolut statement; Hudson Rock / Duel.

[Medium confidenceon the IPO data; motive undetermined — economic and reputational hypotheses both open] — Basis: Economy Magazine (18/09/2026); Financial Times (cited)

Analogous cases — breaches emerging in proximity to listings, acquisitions or share sales. They do not establish a nexus with the Revolut case; they document that, in proximity to extraordinary operations, a security incident produces measurable financial and reputational impacts and that the recurring weak points are late communication and internal anomalies.

Case	Year	Corporate event	Documented impact
Yahoo	2013–14 (revealed 2016)	Acquisition by Verizon	Price cut by 350 mln (4.8 → 4.48 bln); SEC fine 35 mln for late disclosure; class action 117.5 mln
Uber	2016 (concealed until 2017)	SoftBank investment / change of leadership	Concealment; CSO convicted in 2022 for hiding the breach
Equifax	2017	— (listed stock)	Three executives sold shares before the disclosure; SEC/DOJ investigations for insider trading
Coinbase	Jan.–May 2025	Listed company	~69,461 customers; 20-mln extortion refused; estimated cost up to 400 mln; lawsuits over the share drop
Robinhood	Nov. 2021	A few months after the IPO (Jul. 2021)	~7 mln customers; social engineering on a support agent; attempted extortion
Deloitte	2017	Auditor breach → clients' IPO	Peer-reviewed study: an auditor breach in the 90 days before a client's IPO is associated with −4.1% on the offer price (~8.9 mln $ of

			missed capital); effect amplified by media coverage and severity of the breach
Kraken	2025 (lawsuit 2026)	IPO preparation (target Q1 2026, then postponed)	According to the complaint (allegations): data of a highly exposed customer delivered to requests spoofed as Italian authority, without an order; followed by threats, surveillance and attempted entry into the victim's home
Revolut	2022	Before the current listing path	~50,000+ customers; social engineering on an employee; personal data exposed and, in some reconstructions, copies of documents and transaction histories

[High confidenceon the facts of the individual cases; allegations for Kraken] — Basis: Wikipedia/BankInfoSecurity (Yahoo); The Register (Uber); CNN/SEC (Equifax); CoinCentral (Coinbase); Huntress (Robinhood); The Accounting Review — peer-reviewed study (Deloitte); Doe v. Payward filing, Bloomberg (07/03/2025), Fortune (25/09/2025) (Kraken); SecurityWeek/Infosecurity (Revolut 2022).

Outside the strict proximity to an extraordinary operation, other recent episodes document the reputational and market impact of breaches. TalkTalk (2015): on the announcement of the attack the stock lost 10.7% in a single session, followed by a record sanction from the British data-protection authority. UBS and Pictet (2025): an attack on the supplier Chain IQ exposed about 130,000 UBS staff records, which then appeared on a dark-web site, without compromising customer data — a supply-chain risk case. Bank of Baroda (2026): the compromise of an employee's email credentials led to the exposure of customer records, with an incident confirmed by the institution.

[High confidenceon the facts of the individual cases] — Basis: The Register/ICO (TalkTalk); Reuters/SWI swissinfo (UBS–Pictet); The Asian Banker/The Record (Bank of Baroda).

Competitive positioning and international capital

Revolut is by now a systemic player in Italian retail banking: over 5 million customers (May 2026) and the country's fifth bank by number of customers, with transactions of over 50 billion euros (+78% year-on-year) and strongly growing deposits. With the Italian IBAN it has gone from a tool for travel and occasional spending to the main account for many customers ("IBAN effect"). A security incident at an operator of this scale therefore has a direct impact on trust in the banking and fintech system in Italy. Kraken has a different profile — a crypto exchange, not a retail bank — but, serving European Union customers, it falls within the MiCA, AML/CFT and GDPR regulatory perimeter: an incident affects the perception of crypto risk in the EU and investor confidence.

[High confidenceon the market data] — Basis: Il Sole 24 Ore, MilanoFinanza, Teleborsa, Il Giornale d'Italia (Revolut Italy, May 2026); MiCA/AML/GDPR regulatory framework.

[HYPOTHESIS, low confidence] On the geopolitical-economic plane, both Revolut and Kraken are players with strong international capital — Revolut oriented towards a listing on Wall Street as well as in London, Kraken with US roots and a listing path in the United States — that grow by taking market share from the national banking system in retail and investments, with a model based on international capital rather than on local deposits and credit. In this reading, a security incident at operators of this type can also be interpreted as a signal of vulnerability of the fintech model in a phase of reordering of the balance between international capital and national banking systems. It is a contextual key, not an evidential element: no documented nexus emerges between the case and interests of this type, and it must be kept separate from the facts of the incident.

[HYPOTHESIS, low confidence] Reaching a US listing widens, more than the mere adoption of KYC, the perimeter of compliance and exposure: an operator listed in the USA is more sensitive to OFAC requests and to pressure over which assets to list or which users to geoblock, and the policies of the dominant players tend to become de facto global standards — which welds this dimension to the surveillance architecture described later. It is a perspective that touches different interests: cypherpunks read into it a co-optation of crypto by traditional finance; privacy activists, an expansion of financial surveillance; unlisted competitors and DeFi, a regulatory advantage for the big players; part of the regulators and institutional investors, a systemic and reputational risk. These, however, remain grievances and interests — those who are annoyed by a listing — not actors in the case:

none of them appears connected to the incident, and the distinction between those who have an interest and those who acted remains firm.

On the product plane, Revolut positions itself on the border between crypto and traditional banking. In August 2026 it began the rollout of its own euro stablecoin, EURR — legally issued by Bridge, a Stripe company authorised as an electronic-money institution and supervised in Luxembourg, presented as MiCA-compliant — initially to selected customers in Denmark, Poland and Portugal, with integration into the app and on Revolut X. The product is at an early stage (a few hundred tokens in circulation at launch), but the direction is clear: an "internal" crypto asset on a base of over 80 million retail customers, of whom more than 16 million already active in crypto. [High confidence on the facts — Basis: CoinDesk (26/08/2026); The Big Whale; The Paypers]

The regulatory framework accompanies the push: MiCA is finalising the European rules on issuance, guarantees and AML/KYC obligations for stablecoins, and in Europe operators are revising their offering (according to several sources Revolut has reportedly reduced its exposure to Tether/USDT in the EU market). With the Lithuanian banking licence and the US charter under way, Revolut positions itself as a bridge between the crypto world (wallets, stablecoins, trading) and the banking system (accounts, cards, compliance). [Medium confidence on the Tether cut]

For the dossier this is relevant on two planes, with no causal nexus with the attack: (i) it explains why the customer base includes a growing number of crypto "whales" — the target group of the incident; (ii) it raises the compliance and reputational stakes, because an operator that becomes crypto-banking infrastructure and approaches Wall Street is more exposed both to obligations and to reputational damage. The launch of the stablecoin itself has no relation to the compromise of the PEC.

The choice of venue is explicit. Storonsky justified the preference for Wall Street in terms of liquidity: "selling our shares in a small market with few buyers" versus "a giant market with a huge number of suitors", hence the preference to list in the United States before Europe. The reported hypotheses speak of a dual New York–London listing, with Paris as the European hub and a valuation of up to about 200 billion. [High confidence — Basis: Corriere della Sera (21/09/2026); Irish Times, PYMNTS (18/09/2026)]

The choice fits into a broader phenomenon of European "unicorns" migrating towards Wall Street (Flutter, Arm, Spotify, Bending Spoons), driven by greater liquidity and higher valuations: according to the Letta report about 300 billion of European savings a year flow to the United States. The response under discussion in Europe is an aggregation between Euronext (which groups eight exchanges, including Milan, Paris and Amsterdam) and Deutsche Börse — a sort of "European S&P 500" to increase liquidity and retain listings. It is the context in which Revolut's positioning matures: here the stake is not the single incident, but sovereignty over the capital markets and financial infrastructure — the same plane on which trust in the channels and the epigraph's reading of the "27 surfaces" are at play. [High confidence on the facts; connection with the incident not causal — Basis: Corriere della Sera (21/09/2026); Letta report; Euronext–Deutsche Börse, press 09/2026]

Cui prodest — the interests touched

The question that an analysis of this kind cannot evade is cui prodest: who benefits, at this stage, from trust in Revolut being dented. It is not a question of proof — no element emerges linking the incident to a competitor — but of market logic, and as such it must be posed.

Revolut, with over 5 million account holders in Italy, ranks among the top five banking entities operating in the country by number of retail customers, approaching the volumes typical of a systemic operator, and grows while at the same time eroding shares of traditional retail banking deposits, payment and currency-exchange flows, and invested savings, crypto included. Every ground on which it advances is a ground that someone else holds. An incident that strikes precisely the promise on which that growth rests — a secure and reliable digital account — damages not only Revolut: it slows the migration of the more cautious customers towards the fintech model and, by subtraction, benefits those who have the most to lose from that migration. Traditional banks, towards which part of the more conservative clientele may return; competing neobanks, to which the new flows can shift; and, on the crypto-investment front, the vehicles perceived as more institutional.

This last point is the most concrete. In March 2025 BlackRock listed in Europe a physical Bitcoin ETP (IB1T, 0.15% fee), a regulated, exchange-traded product that offers exposure to the cryptocurrency without the investor having to custody a wallet or entrust their documents and keys to a retail app. Between "buying

Bitcoin inside Revolut" and "buying a listed ETP through one's own bank or broker", every episode that reinforces the narrative "on retail apps data is not safe, better the regulated vehicles" shifts value towards the latter. One does not need to imagine orchestration for the effect to occur: the structure of the market is sufficient.

The limit of the analysis remains firm: the competitive motive is structural, not demonstrated. No element indicates an attack orchestrated by a competitor, and this reading must be kept separate from the facts of the incident. But the map of the interests that a case like this touches is itself part of the picture, and for an analysis to ignore it would be a gap.

[Confidence: high on the market facts; the "cui prodest" reading is a structural motive, not demonstrated] — Basis: Il Sole 24 Ore, MilanoFinanza (Revolut Italy); CoinDesk (Revolut 2025 results); Bloomberg, CoinDesk (BlackRock Bitcoin ETP, 03/2025).

So as not to confuse the planes, it is worth distinguishing who acted, who benefits and who makes it a public topic:

Level	Who	Status
Perpetrator (who acted)	Economically motivated crime — in the case, IAmNotAVillain (extortion)	Documented · high confidence
Structural beneficiaries (no evidence of involvement)	Traditional banks and asset managers (trust flowing back from fintech, "regulated" vehicles such as ETPs); competing neobanks; on the geopolitical plane, states (transnational repression)	No evidence of involvement
Voices (those who use the case in the discourse)	Cypherpunk / anti-KYC movement, digital-rights NGOs, the Monero community.	Ideological · non-operational — they are not the perpetrators

Beneficiary and voice do not imply perpetrator: the link is one of method and interest, not of responsibility. The documented perpetrator remains an economically motivated criminal.

14. Patterns that emerged and reconstruction of the operation

Reconstruction of the operation (analytical hypothesis)

1. Access to an institutional PEC mailbox **[Medium-low confidence]** The requests originated from a mailbox on the @pec.interno.it domain that the press attributes to the Local Authorities Office of the Prefecture of Reggio Calabria. Two alternatives remain open: compromise of the mailbox — the hypothesis put forward by the group and by Duel, who speak of credentials stolen via infostealer — or cloning of the address. According to Il Sole 24 Ore (18/09) investigators have no certainty that a computer of the Prefecture or of the Interior Ministry was compromised and are trying to establish whether the mailbox was "breached" or cloned; the Postal Police reportedly has so far found no flaws in the Ministry's systems. A third alternative emerges from The CyberSec Guru (12/09, updated 15/09), according to which the attack allegedly exploited an unauthorised email account created within the government agency's infrastructure; the article presents this as an element confirmed by Revolut, but does not quote its text: it must be verified against the company's official notification or statement. — Basis: press (investigation by the Reggio Calabria Prosecutor's Office); statements by the actor and by Duel; CERT-AGID pattern on compromised PEC mailboxes; Il Sole 24 Ore and ANSA (18/09).

2. Multiple authorities claimed by the same sender **[Medium confidence]** From the same mailbox, communications referencing different authorities were reportedly sent between 4 and 5 May 2026: an EIO in the name of the Public Prosecutor's Office at the Court of Milan, an "Emergency Request for Data Disclosure" and a case referencing "RM-POLPOST". Subject lines and body text are in English with calques from Italian ("European Order of Investigation", "c. ", "att.ne"). — Basis: publicly circulated screenshots of the PEC mailbox and of the EIO document; not independently verified.

3. Anomalies detectable on receipt [Medium confidence] The document lists Lithuania as the executing State and the Lithuanian Prosecutor General and Revolut Bank UAB as recipients, but it was transmitted directly to the PEC of Revolut's Italian branch (revolut.italy.pec@legalmail.it). Direct transmission to the bank, rather than to the competent executing authority of the indicated State, appears incompatible with the normal mechanism for recognition and execution of the EIO (Dir. 2014/41/EU, Art. 9) and should have prompted additional checks. Further elements to verify on receipt: consistency between the issuing authority (a prosecutor's office) and the sender's domain (the Interior Ministry), the signature, use of the standard form (Annex A). On their own, these elements do not prove the document is false — which was, however, subsequently confirmed by Revolut. — Basis: EIO document; PEC screenshots; Directive 2014/41/EU.

4. Handled as routine business [Medium confidence] On 5 May Revolut's Italian PEC replies to the @pec.interno.it mailbox confirming that the documentation was "regularly received" and under analysis, apologises for a "communication misalignment" and opens an internal audit. According to the documents cited by Kozlovska, in July Revolut applies a jurisdictional filter (refusal for Revolut Ltd and for the Swiss entity, 198 hashes), but for accounts held at Revolut Bank UAB it executes the requests, returning encrypted archives with documents, selfies and account data. — Basis: PEC screenshots; Kozlovska's posts of 15 and 16/09 (which do not coincide on this point).

5. Repetition and monetisation [Medium-low confidence] The requests, built on public wallet addresses and transaction IDs, reportedly continued for six months according to the actor and the Italian press, five according to Kozlovska. They are followed by the extortion (first 10,000 BTC, then 6,000 XMR with a countdown), the rift between IAmNotAVillain and Revolut Smilik, Duel putting a "KYC kit" up for sale, and the appearance of sites bearing the group's name. — Basis: Telegram channels; extortion sites; KELA; CoinDesk; the duel.com/merch page; WHOIS.

Patterns

[HYPOTHESIS] 1. The target is the trust channel, not the system. Coinbase (bribed support staff), Kraken 2025 and Revolut 2026 (fake requests from the authorities): in none of these cases is there a breach of the companies' systems. The compromise concerns the outer ring — institutional mailboxes and support personnel — and the attack runs through the procedures in which the company is obliged to cooperate. Exhibits: §§1–3 (summary, chronology, confirmed facts); confirmations from Revolut and Kraken.

[HYPOTHESIS] 2. Little skill, large impact. Institutional-mailbox credentials in circulation; a site built from a template or generated with AI, hosted on free hosting with accessible history (KELA); domains registered in series and taken down within days; a public quarrel between the actors. To obtain KYC data on hundreds of high-net-worth clients, access to a single mailbox is enough. Note: according to investigative sources reported by Il Sole 24 Ore (18/09), investigators consider the operation "very sophisticated"; this assessment diverges from what emerges from the available technical indicators. Exhibits: §4 and §4-bis; KELA; WHOIS records; the site's code; Il Sole 24 Ore (18/09).

[HYPOTHESIS] 3. The attacker learns from the company's responses. Kraken 2025: email, then a fake Irish order when Kraken demands a court. Revolut 2026: in March Revolut points to the Cypriot company for crypto; in May an EIO addressed to Revolut Bank UAB arrives; in July Revolut distinguishes by jurisdiction (Revolut Ltd, the Swiss entity, Revolut Bank UAB). Each formal refusal shows how to package the next request. Exhibits: Kraken complaint paras. 106–108; PEC of 24/03, 04/05, 24/07.

[HYPOTHESIS] 4. From public data to identity, and on to physical risk. [Medium confidence on the selection method; low on the link to concrete assaults] According to the case sources, the fake requests used public wallet addresses and transaction IDs as search keys ("spray and pray"), obtaining documents, selfies and account data in response. The combination of observable blockchain data and exposed KYC data can therefore make it easier to identify and select potential high-net-worth targets. The risk is consistent with the growth in extortions, kidnappings and "wrench attacks" against people connected to cryptocurrencies (the Kraken case; kidnapping threats reported by Duel; personal blackmail of figures in the sector reported by GovInfoSecurity). It is not proven, on the basis of the available sources, that the data stolen in the Revolut case were used in a physical assault. Exhibits: Korra's posts; Kozlovska 16/09; Incrypted 16/09; the wallet-KYC list; §7; GovInfoSecurity.

[HYPOTHESIS] 5. After the incident, the case is put to many uses. Attackers (extortion, ransom reduced to 6,000 XMR with a countdown, the Villain/Smilik split); Duel (contact with the hacker and putting a "KYC kit" containing one

person's document and selfie up for sale); sites bearing the group's name that present themselves as independent sources (.net, .info); security vendors (marketing). Distinct from these self-interested uses, Lyudmyla Kozlovska and the Open Dialogue Foundation — a human-rights organisation — use the case to press for policy reform (FATF, DAC8): a transparent public-interest advocacy position, not an exploitation of the material for private gain. The data keep circulating after the channels are closed. Exhibits: §4-bis, §6.1 and §7; the duel.com/merch page; WHOIS .net/.info.

[HYPOTHESIS] 6. The channel for requests from the authorities has no one accountable for it. The sector invests in transactional fraud, onboarding and crypto (Nasdaq Verafin); verification tools exist but are voluntary (Kodex) or not yet fully operational (e-Evidence, applicable from 18/08/2026, for orders to providers; eEDES, between authorities, with a reference portal in preparation); on 19/09 Interior Undersecretary Wanda Ferro reports in a parliamentary answer that the Ministry's cyber-security structures are conducting further analysis and that the ACN is in dialogue with Revolut; according to the documents cited, Revolut applies jurisdiction checks, not authenticity checks; the debate splits between the company's responsibility and the responsibility of the rules. Exhibits: §8, §8-bis and §13.

In summary. What emerges is not a sophisticated technical attack on Revolut's systems, but the exploitation of a procedure: a real institutional mailbox, plausible documents, knowledge of the group's corporate structure (partly derived from Revolut's own formal replies) and follow-ups to create urgency. The missed control points concern the consistency between the claimed authority and the sender, the EIO transmission circuit, and confirmation of the issuing authority through an independent channel.

14.1 A broader pattern: the abuse of trusted channels

The vector in the Revolut and Kraken cases — a request presented as coming from an authority — is a particular instance of a broader pattern: the abuse of a certified or trusted channel to reach sensitive information about high-value targets. A third case, of a different nature, illustrates it. In 2024–2025 in Italy the Graphite spyware made by Paragon Solutions — a product sold to governments and intelligence agencies — was used to target, via WhatsApp, dozens of people: journalists, activists and, according to reporting by several outlets in October 2025, the financier Francesco Gaetano Caltagirone, a major shareholder in a systemic bank.

Case	Trusted channel	Mechanism	Target and context
Paragon (2024–2025)	WhatsApp, used for private and professional communication	Exploit trust in the channel (chats with known contacts) to deliver zero-click spyware	Surveil sensitive targets: journalists, activists and a major bank shareholder; stakes involving strategic financial assets
Kraken (2025)	An email that looks institutional (law enforcement), with logo and language of authority	Convince the compliance team the request is legitimate and obtain a “whale” client's data	Sensitive financial information, then used for extortion and surveillance; crypto context, large fortunes, EU regulation
Revolut (2026)	A certified PEC on a real state domain	Use a formally perfect channel (aligned authentication) to request customers' KYC and crypto data	“Crypto whale” data, then a ransom demand and threat of a leak; pre-IPO fintech context, market trust

[Confidence: high on the existence of the cases; the “thread” is a pattern of method, not a shared actor or campaign] — Basis: Sky TG24, MilanoFinanza, L’Espresso, TechCrunch, Citizen Lab, Amnesty International (Paragon case); previous sections (Kraken, Revolut).

The common thread is neither an actor nor a campaign, but a method: exploiting the trust placed in a channel — WhatsApp, an institutional email, a PEC — to acquire information on significant targets (activists, bank shareholders, high-net-worth crypto clients), in contexts where control of information has strategic value. A substantial difference must be kept firm: Paragon is a surveillance tool sold to states and agencies, within an authorisation framework, whereas the Kraken and Revolut cases are criminal fraud by impersonation. What they share is only the lever — trust in the channel — not the actor, the legality or the motive.

Yet it is this lever that defines the risk. That a major bank shareholder is surveilled while a contest is being played over control of a systemic institution, and that in the same period crypto exchanges and fintechs are induced to hand over high-net-worth clients' data, draws a coherent picture. For an institution responding to requests from the authorities the lesson is clear: the authenticity of the channel is never, on its own, proof of the legitimacy of whoever uses it.

15. “27 identity wallets”: the reading in the epigraph

The quotation placed at the opening of the dossier — “27 identity wallets = 27 attack surfaces” — reads the EU's 27 member states as so many “identity wallets”: each with its own digital-identity infrastructure (in Italy SPID and PEC; at the European level eIDAS 2.0 and the national wallets), its own authorities (ministries, prefectures, AML units) and its own “trusted” channels (PEC, institutional mailboxes, mutual-assistance portals). Every state is a node of trust in the European architecture; and every node is, at the same time, a potential attack surface.

The Revolut case illustrates the thesis: compromising a single PEC mailbox attributable to an Italian prefecture was enough to deceive a global platform, obtain KYC data on clients from several countries and launch an extortion. It is not the flaw of a single system, but a structural consequence of an architecture that rests on certified national identities, “trusted” inter-state cooperation and KYC platforms required to recognise all these channels. Overall security is not given by the average level of the 27 systems, but by the level of the weakest link that the platforms recognise as legitimate.

On this basis the author of the quotation speaks of “operational sovereignty”: what matters is not declaring 27 European digital identities, but who, in practice, knows how to send a request from an institutional channel and have it recognised as official — whether to protect one's own citizens or to strike an adversary. It is the same mechanism described in §14.1: a state actor need not “attack Europe” if it can compromise a mailbox, or have a third authority forward an apparently legitimate request against a target (cf. the discussion of transnational repression).

[Confidence: the reading “more wallets, more surfaces” and the notion of “operational sovereignty” are the interpretation of the quotation's author, not an established fact; the facts of the Revolut case are dealt with in the relevant sections.]

16. Why Italy

One question remains: why Italy. Not because of a generic weakness, but because of a specific combination of factors. The first is technical. The PEC is a system almost unique in the world: it gives a message the legal value of formal service and certifies sender and delivery, but not who is actually using the mailbox at that moment. A compromised mailbox therefore makes it possible to send formally perfect requests, with aligned authentication. The surface is broad — hundreds of thousands of public and private mailboxes — and little known abroad, where verification teams lack the tools to tell an authentic PEC from an abused one. CERT-AGID handled more than 650 phishing and spam events via PEC in 2026 alone, with more abuse in the first five months of the year than in all of 2025.

The second factor is strategic. Italy is one of Europe's largest banking markets and a laboratory of the Union's financial regulation: from the digital euro — whose preparatory phase at the ECB has concluded, with a launch horizon around 2029 — to the framework on crypto-assets. Obtaining information on major bank shareholders,

on fintech and crypto operators active in Italy and on capital flows means having visibility into banking-consolidation strategies and into Italy's regulatory stance at the European level.

The third factor is internal context: high-tension contests are underway over control of strategic banking assets, in which figures who are at once major shareholders and publishers make digital surveillance a tool for reading moves and alliances and applying pressure. The fourth is one of perception: operating “from Italy”, with real PEC addresses and institutional domains, makes it possible to blend into authentic institutional traffic, to exploit administrative fragmentation to make attribution harder, and to count on the fact that a “made in Italy” incident is downgraded to a local problem when it in fact touches trust in European digital banking and the Union's regulatory debate.

[HYPOTHESIS, low confidence] Lined up, these elements suggest a reading: Italy not as a random victim, but as a platform for access to strategic financial and wealth information, where a technically exploitable certified channel, a leading role in European financial regulation, high-stakes internal contests and an international perception that underestimates Italian risk all combine. It is an interpretive key, not proof: nothing links the cases to a single directing hand, and the three episodes remain distinct in actor, nature and legality.

[Confidence: high on the facts (PEC/CERT-AGID, banking market, digital euro); the overall reading is interpretive, low confidence] — Basis: CERT-AGID (more than 650 PEC events in 2026); ECB (digital euro, 2029 horizon); previous sections.

Financial and wealth information is a strategic asset, and trusted channels (WhatsApp, PEC, institutional emails) are the preferred vectors for acquiring it, lawfully or not.

For Italy, a reputational dimension is added to the technical one. The Revolut case has been absorbed into a broader European narrative about the exposure of institutional leaders' personal data available at data brokers: between September 2025 and September 2026 the press linked analogous episodes in Italy (the phone numbers of Meloni and Mattarella; a €2 million penalty by the Garante against a data broker; the resignation of the ACN director), Germany (Chancellor Merz's number, Der Spiegel), Portugal, Cyprus (President Christodoulides) and Greece. In these accounts — most recently an investigation by To Vima of 19/09/2026 — the common denominator is located in Reggio Calabria, where the researcher who brought many of these cases to public attention operates, and to whose context the Revolut episode is also traced (the compromised PEC mailbox belongs to the Prefecture of Reggio Calabria). [High confidence on the existence of the coverage; medium on the link between the individual episodes — Basis: To Vima (19/09/2026); Der Spiegel (2025); Garante (Jul. 2026)]

This geography must, however, be read with caution: the “Italian origin” is largely an artefact. Many of those episodes were made public by a single Italian source, while the data-broker supply chain is transnational and extra-EU — the platform sanctioned by the Garante is registered in the United States, with an Israeli supplier upstream. Italy is therefore the stage and the media point of contact for the phenomenon, not its source. The reputational risk, for the country, is that the aggregation of Italian markers (a Reggio Calabria mailbox, an Italian contact number, an Italian researcher) makes Italy look like the weak link that exposes Europe, when the data point to a data-market problem of continental scale. [Medium confidence]

[HYPOTHESIS, low confidence] Against this background one can formulate — without evidentiary elements — a reading of the motive alternative to the purely economic one: that the criminal execution (the extortion, real and confirmed) is instrumental to a reputational objective, with Revolut as the primary target and Italy struck on the rebound. In this reading the perpetrator and the beneficiary do not coincide: whoever carries out the attack is not necessarily whoever profits from it. It is a lead to keep open and distinct from the facts: as things stand there is no evidence linking it to a principal, and it must be treated as a hypothesis, not a conclusion. — Basis: analyst's assessment; no documentary corroboration.

Main sources

- Corriere della Sera (21/09/2026); Irish Times and PYMNTS (18/09/2026) — Revolut's US listing and the migration of European “unicorns”; Euronext–Deutsche Börse hypothesis (press 09/2026).
- CoinDesk (26/08/2026), The Big Whale, The Paypers — launch of Revolut's euro stablecoin EURR (issuer Bridge/Stripe, Luxembourg; MiCA context).
- To Vima (Νίκη Λυμπεράκη), 19/09/2026 — investigation into the exposure of institutional leaders' contact details via data brokers; Reggio Calabria context and link to the Revolut case.
- Der Spiegel (2025) — contact details of officials (including Chancellor Merz) obtainable at data brokers; analogous cases in Portugal, Cyprus and Greece.
- Jason Mikula, Fintech Business Weekly, 20/09/2026 — reconstruction of the Revolut case: fake EIOs, executing authority, the Milan/Reggio Calabria contradiction, corporate context.
- Bloomberg (03/09/2026) and OCC (Corporate Decision #1390, Sept. 2026) — conditional approval of Revolut's US bank charter; PYMNTS — IPO not before 2028 (Storonsky).
- Reuters, 12/09/2026 — Revolut confirmation
- Complaint Doe v. Payward Ventures (Kraken), CGC-26-634771 — https://kr-internet-law.sfo3.digitaloceanspaces.com/uploads/Complaint-Doe-v.-Payward-Ventures-Inc-DBA-Kraken-FILED-03.06.26.pdf
- Kraken Security Update (Nick Percoco, CSO Payward/Kraken), X, 13/04/2026 — https://x.com/c7five/status/2043720915330969743; CoinDesk and Unchained, 13/04/2026 (extortion via abuse of internal access)
- The Register, 14/09/2026 — https://www.theregister.com/cyber-crime/2026/09/14/revolut-falls-for-fake-government-requests-hands-over-customer-data/5296118
- StrettoWeb, 15/09/2026 — https://www.strettoweb.com/2026/09/reggio-calabria-hacker-usano-una-pec-della-prefettura-per-rubare-dati-ai-clienti-revolut-indaga-la-polizia-postale/2142679/
- Silere non possum, 15/09/2026 — https://silerenonpossum.com/it/casella-viminale-caso-revolut-ministero-silenzio/
- KELA — https://www.kelacyber.com/blog/revolut-data-breach/
- City AM — https://www.cityam.com/revolut-facing-ransom-request-after-hackers-obtain-customers-data/
- Krebs on Security, FBI e EDR false (11/2024) — https://krebsonsecurity.com/2024/11/fbi-spike-in-hacked-police-emails-fake-subpoenas/
- AML Intelligence, 15/09/2026 — https://www.amlintelligence.com/2026/09/analysis-revolut-breach-puts-renewed-scrutiny-on-fake-law-enforcement-data-requests/
- CERT-AGID, PEC compromesse — https://cert-agid.gov.it/tag/pec/
- HKCERT, Twitter 2020 case — https://www.hkcert.org/blog/case-study-on-bitcoin-scam-incident-a-combined-social-engineering-and-privilege-escalation-attacks
- Security4Web3, 09/06/2026 — https://security4web3.com/blogposts/post33-social-engineering-attacks-crypto
- The Hacker News, Coinbase — https://thehackernews.com/2025/05/coinbase-agents-bribed-data-of-1-users.html
- Yahoo Finance, furto da 282 milioni — https://sg.finance.yahoo.com/news/hacker-steals-282-million-crypto-185613887.html
- Nasdaq IR, comunicati Verafin — https://ir.nasdaq.com/news-and-events/press-releases
- OSCE PA, Dichiarazione dell'Aia 2026 — https://www.oscepa.org/en/documents/annual-sessions/2026-the-hague/declaration-32/5581-the-hague-declaration-eng/file
- franceinfo, PNACO 11/09/2026 — https://www.franceinfo.fr/economie/bitcoin/cryptomonnaies-plus-de-70-enlevements-et-sequestrations-recenses-sur-les-huit-premiers-mois-de-2026-d-apres-le-parquet-national-anticriminalite-organisee_8188352.html

- Potomac Law, e-Evidence — https://www.potomaclaw.com/news-EU-e-Evidence-Rules-Become-Operational-on-August-18-2026-US-Companies-with-European-Operations-Should-Prepare-Now
- Collection dossier “27 identity wallets = 27 attack surfaces” (internal use), with all the sources, screenshots and conflicting versions
- Duel/Korra (X), Kozlovska posts
- Matrice Digitale, Agenda Digitale and the Ministry of Justice circular (for the PEC note)
- Kodex, CoinDesk, Cointelegraph, Chainalysis, Butler Brief
- whoxy/NameSilo,
- European Commission / EUR-Lex.
- Cybernews, 27/07/2026 — announcement of the sale of 75 million Revolut records
- The CyberSec Guru, 12/09/2026 (upd. 15/09) — data categories and the wording of the notification
- IndicePA — digital domicile of the Prefecture of Reggio Calabria (from 12/04/2019)
- PEC lists of the Prefectures, archived versions (Internet Archive, 22/12/2025)
- DDay / Il Sole 24 Ore, 18–19/09/2026 — Postal Police and Cnaipic checks on the 147 GB — https://www.ilsole24ore.com/art/revolut-primi-accertamenti-non-confermano-furto-147-gigabyte-dati-viminale-AJcNmXGB

Hudson Rock, 15/09/2026 — infostealer and compromised pec.interno.it credentials — https://www.hudsonrock.com/blog/revolut-hackers-used-infostealers-for-elaborate-social-engineering

- Corriere della Calabria, 18/09/2026 — answer by Undersecretary Wanda Ferro (ACN, Postal Police, DNAA)
- Economy Magazine, 18/09/2026 — Revolut's listing and valuation (cites the Financial Times)