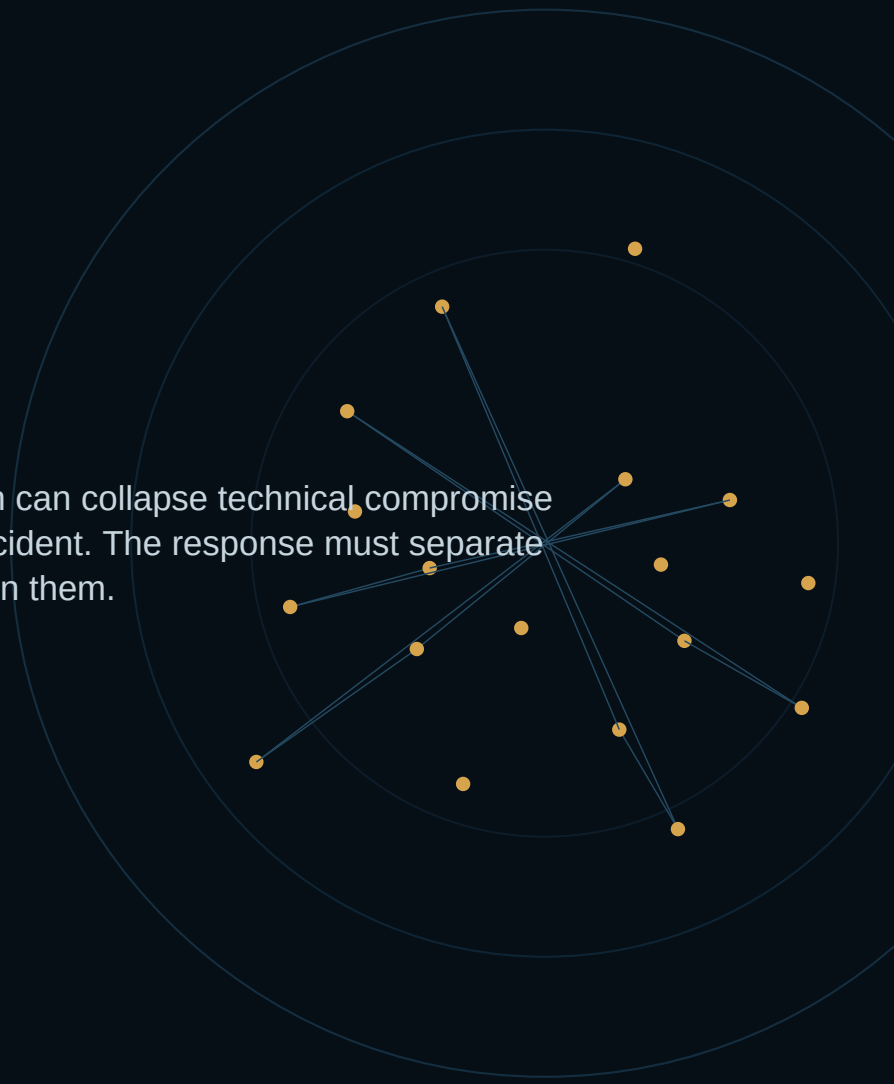
VERIFY CARRATU INTERNATIONAL LTD

INTELLIGENCE / INTEGRITY / IMPACT

DIGITAL IMPERSONATION / INCIDENT RESPONSE PLAYBOOK

The First 24 Hours After Digital Impersonation



A convincing email, voice or domain can collapse technical compromise and financial fraud into the same incident. The response must separate them without creating a gap between them.

RESEARCH & ANALYSIS / JULY 2026

BY VCI / 17 JULY 2026 / 12 MINUTE READ

Verify Carratu International Ltd / Company No. 17327582

carratu.co.uk / ICO Registration: ZC202007

The First 24 Hours After Digital Impersonation

£1.28bn	£1.68bn	429	4,465
reported payment-fraud losses among UK Finance members in 2025 [1]	unauthorised payment fraud prevented by banks in 2025 [1]	incidents requiring NCSC incident-management support in 2024-25 [2]	reports of fake-FCA scams in the first half of 2025 [3]

Digital impersonation succeeds by borrowing trust. The message may appear to come from a managing director, solicitor, supplier, regulator, family member or bank. It may use a compromised genuine mailbox, a lookalike domain, a copied website, a cloned voice or several of those elements at once.

The first day is a contest between four clocks: the movement of money, the persistence of unauthorised access, the volatility of digital evidence and the attacker's ability to approach the next victim. A sequential response is too slow. Containment, financial action, verification and evidence preservation must run in parallel.

Why the incident is both technical and human

The NCSC handled 429 incidents requiring support in the year to August 2025. Of those, 204 were nationally significant and 18 highly significant. [2] Those figures concern incidents reaching the national technical authority, not the full volume of business compromise or fraud.

UK Finance's 2026 Annual Fraud Report records £1.28 billion in payment-fraud losses during 2025 even though banks prevented £1.68 billion of unauthorised fraud. Authorised push-payment losses rose by 19 per cent to £576.4 million, while unauthorised losses fell by five per cent. [1] The divergence matters: a system can authenticate the customer while the attacker controls the story that causes the payment.

That is why password resets alone do not finish an impersonation incident. The organisation must establish which communications were genuine, how the attacker learned the transaction context, which counterparties were exposed and whether another payment or data request is still in motion.

A parallel response timeline

0-30 min	Stop the transaction Call the bank through a trusted number; request recall or freezing action; record transaction identifiers and times.
0-60 min	Contain access Revoke sessions, secure administrator accounts, reset affected credentials, inspect forwarding rules and preserve relevant logs.
First 2 hrs	Authenticate people Contact genuine parties using previously verified details; do not reply to the questioned message or use its telephone number.

First 4 hrs	Preserve evidence Save original emails and headers, messages, call recordings, invoices, domain data, security logs and a decision chronology.
First 8 hrs	Map exposure Identify affected mailboxes, domains, accounts, customers, suppliers, live transactions and information visible to the actor.
Within 24 hrs	Coordinate reporting Consider Report Fraud, police, insurer, regulator, ICO, contractual notices and legal privilege with appropriate advice.
Within 24 hrs	Warn safely Give staff and counterparties one authenticated update route without disclosing details that help the attacker adapt.

WORKED SCENARIO

The invoice was genuine; the instruction was not

A finance team receives an email in an existing supplier thread. The invoice amount, project and sign-off are correct, but the bank details have changed. A follow-up call appears to come from the supplier's finance director and confirms urgency.

The correct analysis keeps several possibilities open: a supplier mailbox may be compromised; the customer's mailbox may be compromised; a lookalike domain may have been inserted; telephone caller ID or voice may be spoofed; or an insider may have supplied transaction details. The true invoice does not authenticate the changed instruction.

The fastest reliable check is an independent callback to a known contact route combined with technical preservation. If the payment has moved, banking action cannot wait for a complete attribution exercise. If access remains compromised, financial recall alone leaves the actor able to repeat the request.

The evidence different teams need

Workstream	Preserve or establish	Frequent mistake
Banking	Payment time, amount, accounts, reference, authoriser and recall contacts	Waiting for a full internal investigation before contacting the bank
Technical	Original messages, headers, sessions, logs, rules, devices and access timeline	Forwarding screenshots instead of preserving originals
Identity	Genuine contact routes, domains, roles, account ownership and connected infrastructure	Assuming the displayed name or caller ID authenticates the person
Legal and regulatory	Decision log, affected data, contracts, reporting duties and privilege position	Circulating speculative blame before facts are established

Workstream	Preserve or establish	Frequent mistake
Communications	Known audience, safe update channel and approved factual wording	Warning people through the same compromised channel

Clone authority works because the real authority exists

The FCA received 4,465 reports of scams impersonating the regulator in the first half of 2025; 480 people reported sending money. [3] A clone firm or regulator does not need to invent credibility. It copies a genuine name, reference number, employee or warning process and changes the contact route.

This produces a counter-intuitive verification rule: finding the real organisation is not enough. The user must compare the domain, telephone number, permissions and contact details with a source reached independently. The FCA's Firm Checker was designed around precisely that distinction.

The same logic applies beyond regulated finance. A copied law-firm site, supplier brand or executive biography can be accurate in every respect except the route through which the victim is communicating.

Controls that make persuasion less decisive

●	Independent callback Require payment changes and exceptional instructions to be confirmed using pre-verified details.
●	Dual control Separate the person creating or changing a beneficiary from the person authorising payment.
●	MFA and session control Protect email, finance and administrator accounts; monitor forwarding and authentication changes.
●	Domain defence Configure email authentication, monitor lookalike domains and retain control of old domains.
●	Low-blame reporting Make it easy for staff to pause a transaction or disclose a click without fear of being blamed.
●	Offline contact book Maintain current supplier, adviser and senior-staff contact routes outside live email threads.

Attribution comes after containment

Domain records, hosting, IP data, social profiles, telephone numbers and payment beneficiaries can generate useful associations. They rarely identify the controlling person on their own. Shared hosting, privacy services, money mules, compromised infrastructure and false documents all complicate attribution.

The investigative questions remain valuable: when was the domain created; what other infrastructure shares identifiers; which public information made the message convincing; did the actor have access to a genuine transaction; and who else may now be targeted? The answers support containment and future decisions even when personal attribution remains uncertain.

A responsible report states confidence, alternatives and technical limitations. Digital investigation should complement qualified incident response and forensics where system access, malware,

evidential imaging or expert testimony is required.

What to carry into the next decision

✓	**Run financial action, technical containment, verification and preservation in parallel.**
✓	**Authenticate the communication route, not merely the name or organisation being copied.**
✓	**Preserve original digital artefacts before they are transformed into screenshots or forwarded messages.**
✓	**Treat infrastructure links as associations unless stronger evidence supports attribution.**

Sources and reading

Sources were accessed and checked for this edition on 17 July 2026. Reported allegations and ongoing proceedings are identified as such in the text.

1. UK Finance. Annual Fraud Report 2026. 11 June 2026. ukfinance.org.uk

2. National Cyber Security Centre. NCSC Annual Review 2025: Incident management. 14 October 2025. ncsc.gov.uk

3. Financial Conduct Authority. Almost 5,000 fake FCA scams reported in first six months of 2025. 27 August 2025, updated 5 December 2025. fca.org.uk

4. Office for National Statistics. Fraud and computer misuse in England and Wales: year ending March 2025. 26 March 2026. ons.gov.uk

5. HM Government. Fraud Strategy 2026 to 2029. 30 April 2026. gov.uk

Scope note

This publication provides general information and analysis. It is not legal, insolvency, financial, regulatory, cybersecurity or other professional advice. Public records and reported material can be incomplete, delayed or disputed; an indicator is not proof of misconduct.

About VCI

VCI provides investigation, intelligence and due diligence support to organisations, professional advisers and private clients. Work is scoped around the decision, the evidence available and the need for proportionate, clearly qualified reporting.