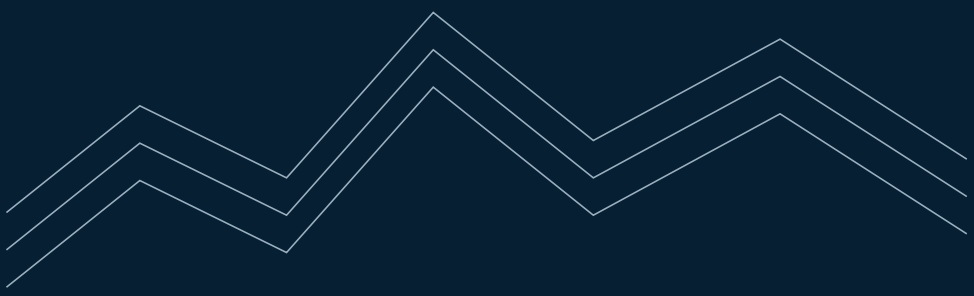
DIGITAL IMPERSONATION · INCIDENT RESPONSE PLAYBOOK

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.

CARRATU INTERNATIONAL / 23 AUGUST 2026



IDENTITY	AUTHORITY	CHANNEL	CONTEXT

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.

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.

Clone authority succeeds 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.

Implications for decision-makers

• 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.

Deepfakes change confidence, not authority

The most important feature of the well-known Hong Kong video-conference fraud was not simply that synthetic video existed. The employee had first received a message purporting to come from a UK-based chief financial officer and was then placed into a conference populated by apparently familiar senior colleagues. Hong Kong authorities said the victim authorised transfers totalling about HK$200 million to five local bank accounts. The fraud succeeded because several cues that normally support trust were assembled into one convincing context. [6]

That distinction matters for senior finance, legal and security teams. Voice, video, email address and apparent seniority can all be evidence of identity, but none should be treated as authority on its own when a request is exceptional. Synthetic media increases the credibility of impersonation; it does not change who is authorised to move money, alter bank details or approve a confidential transaction.

The threat is also no longer confined to isolated demonstrations. Hong Kong Police reported that deception accounted for 46.9% of recorded crime in 2024 and described subsequent criminal groups using deepfake technology in fraud. The relevant risk is therefore organisational: attackers can combine publicly available media, compromised

communications and social knowledge to make an instruction look internally coherent. [7]

The channel is part of the persuasion

Impersonation fraud increasingly exploits the authority attached to normal business systems. A request arriving through an email thread, messaging platform or familiar video-conference environment inherits some of the trust users place in that channel. If an account has been compromised, or a convincing look-alike identity has been inserted into an existing process, the message may contain all the contextual details that generic fraud awareness training tells staff to look for.

This is why visual quality is a weak dividing line between genuine and false communications. The stronger question is whether the requested action is consistent with independently established authority, commercial context and normal controls. A technically convincing message can still be anomalous because it changes beneficiary details, compresses decision time, bypasses a colleague, invokes unusual secrecy or combines several departures from ordinary practice.

For incident analysis, that also means the first visible fraudulent message may not be the beginning of the event. Earlier access to an inbox, calendar, supplier conversation or shared document can provide the information needed to construct a credible later instruction. The fraud and the compromise are related propositions, but they are not necessarily the same event.

Real-world context: Arup and the deepfake conference call

In 2024 engineering group Arup confirmed that an employee in Hong Kong had been deceived into transferring HK$200 million after a video conference in which criminals used digitally generated representations of senior colleagues. The incident demonstrates why familiar faces and voices can no longer be treated as sufficient authentication for an exceptional payment instruction.

Public source: Arup incident as reported by the Financial Times and confirmed publicly in May 2024.

Sources and reading

Sources were accessed and checked for this edition on 23 August 2026. Reported allegations and ongoing proceedings are identified as such in the text.

1. 1**UK Finance.** Annual Fraud Report 2026. 11 June 2026.
2. 2**National Cyber Security Centre.** NCSC Annual Review 2025: Incident management. 14 October 2025.
3. 3**Financial Conduct Authority.** Almost 5,000 fake FCA scams reported in first six months of 2025. 27 August 2025, updated 5 December 2025.
4. 4**Office for National Statistics.** Fraud and computer misuse in England and Wales: year ending March 2025. 26 March 2026.
5. 5**HM Government.** Fraud Strategy 2026 to 2029. 30 April 2026.
6. 6**Hong Kong Government.** LCQ9: Combating frauds involving deepfake. 26 June 2024.
7. 7**Hong Kong Government.** Law and order situation in Hong Kong in 2024. 11 February 2025.

Scope note

This article 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.

Carratu International

About the author

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