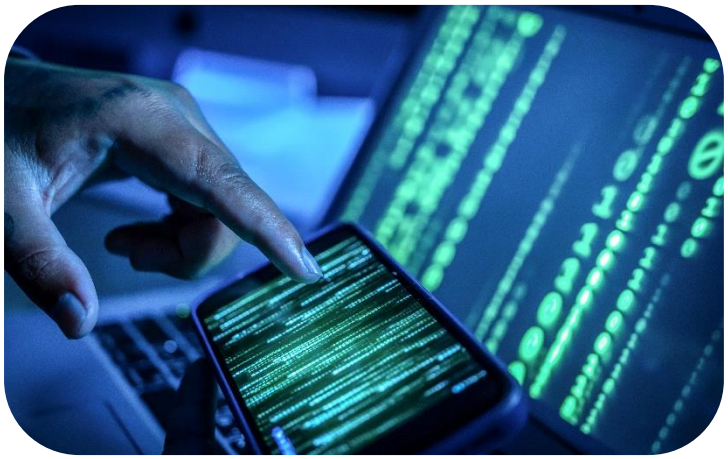
Social Engineering Fraud – SIM-Swap and Ghost Pairing

This Loss Prevention Standard provides clear and practical guidance to help protect authentication processes, prevent account takeover and safeguard your organisation from fast-moving, high-impact social engineering attacks.

Version: 1.0
Date: 29th May 2026

Social Engineering Fraud – SIM-Swap and Ghost Pairing

Introduction



Companies are facing increasing exposure to the next iteration of social engineering fraud: identity takeover.

This threat is being driven by the rapid growth of telecommunications-based attack methods, particularly SIM-swap fraud and ghost pairing, which enable attackers to compromise identities and subsequently conduct targeted social engineering attacks.

Both SIM-swap fraud and ghost pairing exploit vulnerabilities within telecommunications providers, enabling criminals to hijack a victim's mobile identity, intercept calls and SMS messages, and bypass SMS-based two-factor authentication (2FA) and multi-factor authentication (MFA) controls. This can result in high-impact account takeovers and significant financial losses.

SIM-swap fraud is rapidly accelerating, with UK cases rising with a 1,055% surge in unauthorised SIM swaps in 2024 and nearly half of account takeover incidents now involving mobile numbers.

Attacks use these techniques for a number of reasons, including:

- Reliance on SMS-based authentication for banking and system access.
- Weak telecom verification processes, easily manipulated via social engineering.
- Lack of SIM-swap alerts or delay mechanisms.
- Low internal prohibition on using personal numbers for corporate access.
- Insufficient training and awareness on telecom-enabled fraud.
- Unsecured executive communications, enabling social engineering entry points.

Research shows criminals increasingly operate across multiple channels, e.g., email → social media Apps → mobile takeover, to build credibility and exploit urgency, leading to CEO impersonation schemes, business email compromise, social media account hijacking, internal payment fraud, and unauthorised fund transfers.

Note: SIM is an abbreviation of Subscriber Identity Module, a small, chipped card, in a mobile device, that stores the owners identity and connects to a mobile network.

What is Sim-Swap Fraud?

SIM-swap is a fraud typology that allows an attacker to hijack a person's mobile phone number and use it to bypass security protocols. Once the attacker gains control, they can access sensitive accounts from emails to banking details, with little more than a phone number and some social engineering techniques.

SIM-swapping occurs when the attacker impersonates the victim, provides personal details and tricks the customer service representative of the mobile carrier into executing the switch.
The key stages in enabling SIM-swap fraud include:

- Gathering the victim's personal data, typically via social media, phishing, or data breaches.
- Impersonating the victim to the mobile provider and requesting a SIM swap.
- The victim's phone loses signal, and the attacker gains control of SMS, calls, and one-time passcodes (OTPs).
- Initiating password resets, with verification codes sent via SMS to the compromised number.
- Taking full control of the victim's mobile number, enabling access to:
  - ✓ SMS OTPs.
  - ✓ MFA / 2FA prompts.
  - ✓ Password reset messages.
  - ✓ Voicemail (often overlooked).
  - ✓ Incoming calls intended for the victim.

SIM-swap fraud often happens without any compromise of the company's systems. It is attractive due to its high payout and low technical requirement and is now one of the most damaging telecom-related fraud schemes globally.

What is Ghost Pairing Fraud?

Note: This section discusses IMSI, an abbreviation of International Mobile Subscriber Identity, the digital identity of a SIM card on the mobile network.

Ghost pairing refers to the cloning or duplication of SIM authentication credentials (IMSI and authentication keys), allowing attackers to connect to the mobile network as a "ghost" duplicate of the legitimate SIM. Key characteristics include:

- The victim's phone remains active, unlike in a SIM swap scenario.
- The attacker covertly receives copies of calls, and SMS, and can use the victim's identity on another device.
- It enables persistent, stealthy access, making detection extremely difficult.
- Security research indicates that attackers exploit weaknesses in telecom processes to attach rogue devices to a victim's mobile identity.

Ghost pairing is typically used for:

- Long-term surveillance.
- Intercepting 2FA codes.
- Reinforcing impersonation fraud (including CEO fraud).
- Corporate espionage.
- Covert access before executing larger financial attacks.

Ghost pairing, while less publicly discussed, is becoming increasingly sophisticated and does not alert the victim.

How can These Affect Businesses?

Allowing employees to use their personal phones for business use is an often-overlooked risk. Commonly, personal phones provide:

- MFA to corporate email, VPNs and finance systems.
- Banking or payment approvals.
- Social Media, Apps, SMS with colleagues and suppliers.
- Calendar access (revealing timing, travel and approval windows).

As a result, the distinction between work and personal devices becomes blurred and a personal phone becomes a trust anchor (a known, trusted starting point used to verify identities, certificates, or systems) between the individual and the company.

A number of high-profile reported SIM-swap incidents have resulted in the compromise of internal business systems. In these cases:

- Employee credentials were obtained via social engineering.
- A SIM swap enabled criminals to bypass 2FA controls.
- Unauthorised access to internal systems was gained, resulting in data breaches and/or financial loss.

Case Study One

A finance manager at a large firm had their personal mobile number SIM-swapped after an attacker collected basic open-source intelligence (OSINT) data from a professional social networking platform.

Once the attacker controlled the mobile number, they reset the victim's corporate email password and intercepted MFA codes.

Using the finance manager's mailbox, the attacker sent an email to the business's Accounts Payable team referencing a live project and payment of legitimate invoices. They advised the Accounts Payable team that the supplier's bank account details were changing "to comply with SEPA" and attached a forged letter to this effect

Note: SEPA is an abbreviation of Single Euro Payments Area, a legitimate business process to comply with European payment standards, reported to have been used in fraudulent payment redirection.

The Accounts Payable team completed a call-back to the compromised mobile number, which the attacker answered convincingly to authorise the payment. A £1.2m payment was then sent to the criminal's account.

Case Study Two

A regional HR director used their personal phone for a payroll approval MFA. After a SIM swap, the attacker accessed the director's personal email account, which held payroll correspondence and approval templates. The attacker then submitted a request to change the salary bank details for eight senior staff members.

Because the request appeared to come from the director's mailbox, and the associated MFA appeared legitimate, payroll processed the changes, leading to significant losses.

How These Incidents Typically Materialise

Step 1. SIM swap on the employee. The attacker socially engineers the mobile provider and ports the number to a new SIM.

Step 2. Account takeover using trusted channels. With control of the number, the attacker can:

- Reset corporate email passwords.
- Pass SMS-based MFA.
- Access personal email that contains work correspondence.
- Retrieve voicemail messages confirming transactions or instructions.

At this point, the attacker can observe tone, language, approval processes, and authority structures to aid in fraud facilitation.

Step 3. Social engineering attack from a trusted identity. Now the attacker impersonates the employee using:

- A genuine email account.
- A known mobile number.
- Familiar writing style and timing.

This bypasses many controls because the request appears:

- Legitimate.
- Authenticated.
- Internally validated.

Step 4. Loss crystallises at company level. The funds move from the company's account, not the employee's. Therefore, although the initial compromise is personal, the resulting financial loss is suffered by the corporate entity.

Key points to recognise:

- No malware required.
- No system vulnerability exploited.
- Controls fail because they trust the identity, not the process.

The fraud succeeds because:

- The organisation trusts the identity, not just the system.
- Controls rely on SMS-based assurance.
- Verification is often circular ("we checked with the same number").

How can the Risks be Managed?

Education is key, ensure all staff are aware of this risk and consider adopting the following procedural controls:

1. Strengthen Authentication (Move Away from SMS-Based MFA)

- Use authenticator apps instead of SMS.
  - ✓ E.g., Microsoft Authenticator, Google Authenticator, Duo. These are *not* tied to a phone number and cannot be intercepted through a SIM swap.
- Use push-based MFA with device binding.
  - ✓ Ensures approval can only come from a previously trusted device.
- Implement conditional access / behavioural monitoring.
  - ✓ If a login comes from a new device or location, require extra verification.

2. Harden Payment, Payroll, and Supplier Change Controls

- Call-backs using a verified number - A "verified number" is a phone number obtained from an internal system or independent trusted source (e.g., a contact number sourced from the supplier's official website), established before the request, and not influenced by the communication asking for the change. Never rely on:
  - ✓ "The number in the email signature".
  - ✓ "The number used before".
  - ✓ "The number provided in the request".

  Instead, use a directory-stored number or a known supplier record.
- Require two-person verification for all bank-detail changes.
  - ✓ One person validates the change; another independently verifies the "why".
- Block approvals via personal SMS.
  - ✓ Move toward corporate-controlled approval channels or secure workflow systems.
- Enforce 'cooling-off' periods.
  - ✓ When bank details are updated (supplier or payroll), flag high-risk payments for manual review for a specific number of days.

3. Protect Email & Identity: Make Account Takeover Harder

- Enforce MFA on ALL corporate email accounts.
  - ✓ Ideally app-based, not SMS.
- Use "unfamiliar sign-in" alerts.
  - ✓ A SIM swap followed by a new login often triggers abnormal patterns.
- Require password resets via secure channels only.
  - ✓ Disable SMS-based resets for senior staff or finance roles.

4. Manage the Human Layer (Awareness & Behaviour)

- Employee training on SIM swap indicators and ghost pairing. Teach staff to escalate immediately if they notice:
  - ✓ Sudden loss of signal.
  - ✓ New SIM activation text.
  - ✓ Unexplained MFA prompts.
  - ✓ Mobile provider "account change" alerts.
  - ✓ Unusual activity.
- Educate on the risk of using personal numbers for work MFA.
  - ✓ Encourage migration to app-based alternatives.
- Encourage staff to use account PINs with mobile providers.
  - ✓ Most telecom networks allow a porting / swap PIN that blocks unauthorised swaps.

5. Implement Executive-Specific Controls (High Risk Area)

- Separate executive approval channels for high value payments, e.g., no high-value payment approvals via email + SMS alone. For example:
  - ✓ Hardware based approval from the executive requesting (e.g., YubiKey, Onlykey, Google Titan Security Key, etc.).
  - ✓ Banking or Treasury system-based approval.
  - ✓ Requirement of another executive independent approval.
  - ✓ In-person or video call to authorise.

- Provide corporate-secured devices.
  - ✓ Even if employees prefer using personal phones — finance approvals should be restricted to business phones only.
- Apply stricter monitoring on exec email accounts.
  - ✓ Attempts to reset passwords or MFA prompts should trigger alerts.

6. Telecom-Level Protections (Often Overlooked)

- Corporate mobile contracts with enhanced security. Many carriers offer:
  - ✓ SIM swap delay windows.
  - ✓ Swap confirmation via multiple channels.
- Fraud flags after suspicious port-out requests.
- Mandate port-out protection features for senior staff.
  - ✓ Especially CFO, CEO, finance managers, treasury roles.

7. Incident Response Preparedness

SIM swap usually gives attackers hours, not days. Ensure the following are in place:

- Rapid account lockdown process.
  - ✓ Employees should know exactly who to call the moment they suspect an issue.
- Payment suspension protocol.
  - ✓ If a SIM swap is suspected, freeze certain activities across the business could assist, including:
    - Supplier bank changes.
    - Pending approvals.
    - Payroll changes for that individual's authority.
    - Pre-set contacts with telecom providers.
- Faster response can result in lower losses.

Contact Information

United Kingdom

Please visit Aviva Risk Management Solutions or email us at riskadvice@aviva.com. To speak to one of our advisors, call 0345 366 6666.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

Canada

Please visit Aviva Risk Management Solutions | Aviva Canada or email us at arms.canada@aviva.com

Ireland

Please visit Insurance Risk Management | Business Risk Management Insurance - Aviva Ireland or Email us at armsireland@aviva.com

Specialist Partner Services

Aviva have created a network of Specialist Partners to complement our in-house capabilities and to enable our policyholders to benefit from a wide range of risk management solutions at preferential rates and terms. Together, we provide solutions to help with the significant challenges of modern-day risk management.

Note: These partner relationships are wholly for the benefit of our policyholders with no income to Aviva.

The following Specialist Partners provide products or services in relation to risk guidance provided, discussed or referenced in this Loss Prevention Standard.

United Kingdom

For more information please visit: Aviva Risk Management Solutions – Specialist Partners

Ireland

For more information please visit: Insurance Risk Management | Business Risk Management Insurance - Aviva Ireland

Canada

For more information please visit: Our Specialist Partner Network | Aviva Canada

Standards, Sources and Useful Links

Canada

- Canadian Anti-Fraud Centre
- National Cybercrime and Fraud Reporting System

Ireland

- National Cyber Security Centre

United Kingdom

- Credit Industry Fraud Avoidance System
- National Fraud Intelligence Bureau

Other

- Internet Crime Complaint Center

Additional Information

Loss Prevention Standards

These documents set out best practice recommendations to help reduce the likelihood and impact of losses.

Relevant Aviva Loss Prevention Standards include:

- **Payee Verification Policy**
- **Social Engineering**

Please visit Loss Prevention Standards to view the full library.

Aviva Risks Training Solutions (United Kingdom Only)

Aviva Risk Training Solutions, delivered through our Specialist Partner, SafetyCulture, provide free, bite-sized learning modules exclusively for Aviva policyholders.

Please visit Aviva Risk Training Solutions for further guidance.

29th May 2026

Version 1.0

ARMSGI4202026

Aviva Insurance Limited, Registered in Scotland Number SC002116. Registered Office: Pitheavlis, Perth PH2 0NH.
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.