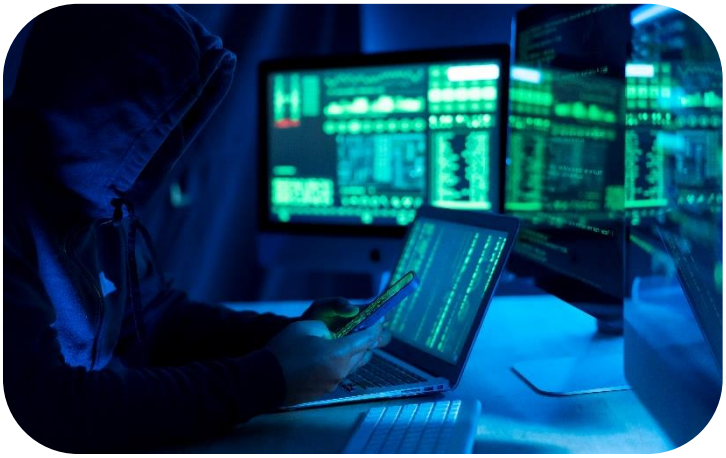
Lessons from the 2025 UK Retail Cyber-Attacks

This guidance has been written to highlight the tactics, techniques and procedures used in several high-profile cyber-attacks in the first half of 2025, as well as the practical steps that businesses can take to mitigate the likelihood and impact of attacks.

Version: 1.1
Date: 19th August 2025

Lessons from the 2025 UK Retail Cyber-Attacks

Background



In the first half of 2025, several high-profile attacks were propagated against a number of well-known retailers in the United Kingdom. The quick succession and impact of the attacks heightened public awareness of cyber security and raised urgent concerns about the growing threat of cyber-attacks compared with the sector's cyber resilience.

This Loss Prevention Standard has been written to highlight the tactics, techniques and procedures used by the alleged threat actors, as well as the practical steps that a business can take to mitigate the likelihood and impact of attacks.

A Sector Under Scrutiny

The National Cyber Security Centre (NCSC) has confirmed it is working closely with all affected retailers to assess the nature of the attacks and provide guidance to the wider sector. Richard Horne, NCSC's chief executive, described the incidents as a "wake-up call" for the industry.[1] Experts have pointed to the increasing use of social engineering—including phishing, impersonation, and manipulation of remote work tools—as a key vector in these attacks.

They have also provided a write-up on the incidents and some additional recommendations: Incidents impacting retailers – recommendations from the NCSC - NCSC.GOV.UK.

Scattered Spider

Scattered Spider (also known by the aliases UNC3944, Starfraud, Muddled Libra, and Scatter Swine) is a financially motivated cybercriminal group. Known for its aggressive and sophisticated social engineering and identity-centric attacks, the group has targeted major enterprises across various sectors including telecommunications, finance, retail, and critical infrastructure. Their operations are marked by a deep understanding of identity systems, cloud environments, and endpoint security tools. They are believed to be behind some, if not most, of the high-profile attacks on the UK retail sector.

Initial Access - Social Engineering at Scale

Scattered Spider are known for their sophisticated and multi-layered social engineering tactics, which are designed to exploit human trust and procedural weaknesses rather than technical vulnerabilities. These methods are often deployed together, creating a higher probability of success even in organisations with mature security postures.

[1] NCSC Statement: Incident impacting retailers - NCSC statement: Incident impacting retailers - NCSC.GOV.UK

Phishing and Smishing

The group initiates many of its campaigns through phishing emails and SMS-based phishing (smishing). These messages are not generic spam—they are highly tailored, often using spoofed domains under the ownership of the group that closely resemble legitimate corporate infrastructure (e.g., victimname-okta.com, victimname-sso.com).

The content typically mimics internal IT communications, such as password reset requests or MFA re-enrolment notices, whilst directing users to credential harvesting portals that replicate familiar login interfaces.

These phishing sites are often hosted on infrastructure that appears benign or is newly registered to avoid detection. The attackers may also time these messages to coincide with known IT events (e.g., scheduled maintenance) to increase credibility.

In parallel with phishing, Scattered Spider also employs vishing—a tactic where attackers call employees directly, impersonating IT support or helpdesk personnel. These calls are often well-scripted and convincing, leveraging publicly available information (e.g., LinkedIn profiles, company org charts) to personalise the interaction, as well as using company specific terminology (e.g. referring to internal systems)

The goal is typically to:

- Convince the target to share a one-time MFA code.
- Persuade them to install a remote access tool under the guise of troubleshooting.
- Gain enough trust to escalate privileges or reset credentials.

Even well-trained employees have fallen victim to these calls due to the attackers' professionalism and urgency.

SIM Swapping

To bypass MFA, Scattered Spider have been known to use SIM swapping. This involves socially engineering telecom providers into transferring a victim's phone number to a SIM card controlled by the attacker. Once successful, the attacker can intercept SMS-based MFA codes and password reset links.

This technique is particularly effective against executives, IT administrators, and other high-value targets whose accounts are protected by SMS-based MFA. It also enables attackers to take over accounts silently, without triggering alerts that might accompany phishing attempts.

It's also worth noting that even firms that utilise push-based MFA applications, like Microsoft Authenticator or Duo, are at risk of breaches through something known as MFA fatigue. Attackers initiate a flood of MFA push notifications to the user's device. The goal is to exploit user behaviour—many individuals, when overwhelmed or distracted, will eventually approve the request out of frustration.

These techniques are rarely used in isolation. Scattered Spider often combines phishing, vishing, and SIM swapping in a coordinated campaign, increasing the likelihood of breaching initial defences. For example, a phishing email may be followed by a vishing call to "verify" the request, while a SIM swap ensures uninterrupted access to MFA tokens.

Gaining and Maintaining - Post initial access persistence

Another key element of Scattered Spider's approach is their use of legitimate, commercially available tools to maintain access, move laterally, and exfiltrate data—while minimising their footprint and evading detection. This "living-off-the-land" (LOTL) approach allows them to operate within the boundaries of what appears to be normal administrative behaviour, making traditional security controls less effective.

Remote Monitoring and Management (RMM) Tools

Scattered Spider frequently deploys remote access and RMM software that is commonly used by IT administrators and managed service providers. These include:

- ScreenConnect
- Splashtop
- Pulseway
- Tactical RMM
- Tailscale
- TeamViewer
- Fleetdeck.io
- Level.io

These tools are often installed by tricking users into believing they are receiving legitimate IT support (e.g., during a vishing call). Once installed, they provide full remote control over the system, including file access, command execution, and lateral movement capabilities.

Because these tools are signed, trusted, and widely used, they often bypass endpoint protection and are not flagged as malicious. This can make them ideal for stealthy persistence and control.

Living-Off-the-Land (LOTL) Techniques

Beyond third-party tools, the group also leverages native system utilities and allow listed applications to avoid detection. Examples include:

- PowerShell and WMI for command execution and system reconnaissance.
- Built-in VPN clients to route traffic through trusted channels.
- Endpoint Detection and Response tools already present in the environment, which they repurpose for remote shell access and command execution.

This LOTL strategy enables them to blend in with legitimate administrative activity, making it difficult for defenders to distinguish between benign and malicious behaviour.

By abusing tools that are already trusted within the environment, Scattered Spider reduces their reliance on custom malware, lowers the risk of detection, and increases the complexity of incident response. Their ability to weaponize legitimate software and infrastructure is a key reason why they remain such a persistent and dangerous threat.

The Australian government has put together a good write-up on LOTL techniques, and best practices for mitigating against them: Identifying and Mitigating Living Off the Land Techniques | Cyber.gov.au.

Stealing Data, Ransomware Deployment, and Long-Term Persistence

With access gained and easily accessible, Scattered Spider begin to go much further—quietly gathering valuable information, foot printing an organisations infrastructure, locking up systems with ransomware, and demanding payment to stop the damage or keep stolen data private.

One of their first moves is to collect any sensitive data they can access. Things like customer records, internal documents, and login details. They gather this information in one place, then send it out to cloud storage services they control, (such as MEGA.NZ). This often happens before they do anything else, so they already have something to threaten the company with.

In some cases, they go a step further and install ransomware. This is a type of software that locks up important systems, especially servers that run virtual machines, like VMware ESXi or Proxmox. The attackers then demand a ransom to unlock the systems. This "double threat" approach (stealing data and locking systems) puts extra pressure on the company to pay up.

To make sure they can maintain persistence inside a company's systems for as long as possible, they use several tricks. They might register new devices for multi-factor authentication, create fake user accounts, or change settings that allow them to keep logging in—even if passwords are changed. They've also been observed taking time to explore the company's network, looking for things like backup systems, shared files, and software code that might be useful or valuable. They've even been known to join incident response and recovery calls to understand what steps the organisation is taking to contain, eradicate and recover.

Important: In the event of a compromise, it's advisable that organisations use clean IT systems and messaging apps to conduct recovery activities and communications.

Mitigations

Scattered Spider's operations exploit a blend of social engineering, identity abuse, and legitimate tool misuse. To effectively reduce the risk posed by this threat actor, organisations must adopt a layered defence strategy that integrates identity hardening, remote access governance, behavioural monitoring, and incident readiness. The advice below has been taken from the US-based Cybersecurity & Infrastructure Security Agency's guide on Scattered Spider, and their guidance on Securing remote access software and Implementing Phishing resistant MFA.

1. Implement Phishing-Resistant Multi-Factor Authentication (MFA)

Given scattered spider's advanced use of social engineering techniques, it's strongly recommended to adopt phishing-resistant MFA as the most effective defence against credential-based attacks. While any MFA is better than none, not all MFA methods offer equal protection.

- Prioritise FIDO2/WebAuthn or PKI-based MFA. These methods are resistant to phishing, SIM swapping, and push bombing attacks. FIDO2 tokens can be hardware-based (e.g., USB keys and Yubi Keys) or embedded in devices, while PKI-based MFA (e.g., smart cards) is suitable for large, mature environments.
- Avoid SMS and basic push-based MFA. These are vulnerable to interception and social engineering. If required, they are best used on low-risk systems.
- Where push-based notifications to an application are used, implement number matching (e.g. select the matching number identified at the login page from three options presented on the mobile application) to reduce the risk of accidental approval.
- Phase implementation based on risk. Begin with high-value targets such as IT administrators, executives, and helpdesk staff. Expand coverage in stages, using lessons learned to inform broader rollout.
- Identify systems that do not support modern MFA and develop a roadmap to upgrade or replace them. Where immediate replacement is not feasible, apply compensating controls such as strict network segmentation and enhanced monitoring.

2. Monitor and Secure SSO and Identity Provider (IdP) Configurations

Scattered Spider has demonstrated a deep understanding of identity infrastructure, often exploiting weaknesses in single sign-on (SSO) and federated identity setups. To reduce this risk:

- Regularly audit federated identity providers in systems like Okta, Azure AD, and similar systems. Look for unexpected additions or changes to trusted Identity Providers (IdPs).
- Disable unused or suspicious IdPs and enforce strict attribute mapping to prevent unauthorised account linking or impersonation.
- Monitor for unauthorised changes to authentication flows, MFA settings, or SSO configurations. Set up alerts for changes to identity federation settings or new MFA device registrations.

3. Enforce Strong Password Policies

MFA is critical, but strong password hygiene remains a foundational control. Threat actors often use databases of common passwords from other data breaches in programs that they've written to try against exposed login pages. Following NIST SP 800-63B[2] guidelines can help to reduce the risk of brute-force and credential stuffing attacks:

- Require passwords to be a minimum of 16 characters, using a mix of random and unique characters. Avoid periodic password resets unless there is evidence of compromise. Frequent resets can lead to predictable patterns.
- Encourage the use of enterprise-standard password managers to support the creation and secure storage of strong, unique passwords.
- Prohibit password reuse across systems, especially privileged or administrative accounts.

4. Control and Monitor Remote Access

Remote access tools are essential for IT operations but are frequently exploited by threat actors. Proper governance and monitoring are key to reducing the likelihood and magnitude of exploitation.

Application Allowlisting

- Implement application control policies to block unauthorised software, especially portable or self-contained remote monitoring and management (RMM) tools.
- Maintain a list of approved remote access tools and block all others by default, including those that can run without installation.

Audit and Restrict RMM Usage

- Identify all RMM tools in use (e.g., ScreenConnect, Splashtop, Tactical RMM) and validate their necessity.
- Require RMM access only through secure channels such as VPNs or virtual desktop infrastructure (VDI).
- Monitor logs for unexpected RMM activity, particularly outside of standard working hours or from unusual locations.

[2] Digital Identity Guidelines - NIST Special Publication 800-63B

Limit RDP and Remote Desktop Services

- Disable Remote Desktop Protocol (RDP) where not strictly necessary.
- If RDP is required:
  - ✓ Enforce Phishing Resistant MFA for all RDP sessions.
  - ✓ Log all access attempts and monitor for anomalies.
  - ✓ Apply account lockouts after a defined number of failed logins attempts to prevent brute-force attacks.

5. Strengthen Detection and Response Capabilities

Early detection and rapid response are critical to limiting the impact of an intrusion. Organisations should invest in tools and processes that provide visibility across endpoints, identities, and network activity, with appropriate personnel ideally reviewing the outputs of these systems on a 24/7 basis.

Deploy and Tune EDR/XDR Solutions

- Ensure endpoint detection and response (EDR) or extended detection and response (XDR) tools are deployed across all critical systems. These systems should be configured to automatically identify suspicious activities such as:
  - ✓ Credential dumping tools.
  - ✓ Logons from unusual locations.
  - ✓ Unusual remote shell activity or command-line execution.
  - ✓ Use of legitimate administrative tools in suspicious contexts.

Monitor for Identity Abuse

- Set up alerts for identity-related anomalies, including:
  - ✓ Multiple MFA prompts in a short period (indicative of MFA fatigue attacks).
  - ✓ New MFA device registrations or changes to authentication settings.
  - ✓ Modifications to SSO or IdP configurations.

Conduct Threat Hunting

- Proactively search for indicators of compromise (IOCs) associated with Scattered Spider, including known infrastructure such as MEGA.NZ or Ngrok tunnels.
- Investigate abnormal user behaviour, such as logins from unexpected locations, devices, or at unusual times.
- Use threat intelligence feeds to stay updated on evolving tactics and infrastructure.
- The UK Government has produced guidance on threat hunting that can be found at the following link: Detecting the Unknown - A Guide to Threat Hunting

6. Prepare for and Limit the Impact of Intrusions

Even with strong defences, no system is immune to compromise. Organisations must be prepared to respond effectively and recover quickly.

Maintain Offline, Immutable Backups

- Store backups in physically separate or cloud-isolated environments that are not accessible from the main network.
- Ensure backups are encrypted and immutable (i.e. they cannot be altered or deleted once written).
- Regularly test backup restoration procedures to ensure data can be recovered quickly and reliably.

Segment Networks

- Isolate critical systems such as domain controllers, backup servers, and cloud management consoles from general user access.
- Use firewalls, VLANs, and access control lists to restrict lateral movement within the network.
- Apply zero-trust principles where possible, verifying every access request regardless of origin.

Implement a Recovery Plan

- Develop and maintain an incident response plan that includes:
  - ✓ Scenarios involving identity compromise and cloud infrastructure breaches.
  - ✓ Procedures for ransomware containment and data recovery.
  - ✓ Consider how the organisation will recover against a deliberately destructive attack. If your active directory infrastructure and all laptops are wiped, how would you react as an organisation?
  - ✓ Communication protocols for internal stakeholders and external partners, including legal, regulatory, and public relations considerations.
- Conduct regular tabletop exercises and simulations to validate the plan and improve team readiness.

7. Educate and Empower Users

Arguably, the most critical element in this list for reducing the likelihood of a successful attack. Human error remains one of the most common entry points for attackers. Building a security-aware culture is essential to reducing risk.

Security Awareness Training

- Provide regular training to all staff on how to recognise:
  - ✓ Phishing and smishing messages.
  - ✓ Vishing attempts, such as fake IT support calls.
  - ✓ AI generated fake videos and voicemails.
  - ✓ MFA fatigue attacks and how to respond appropriately.
- Tailor training for high-risk roles such as executives, IT administrators, and helpdesk personnel.

IT Helpdesk Verification Protocols

- Require multi-step identity verification before processing any password resets or MFA re-enrolments. Ideally performing in person or with video calls with all cameras on.
- Implement audit logging for all helpdesk actions related to identity and access management.

IT Helpdesk Staff training

Staff in these roles are likely to be targeted by sophisticated social engineering attacks. Some indications that the call could be phishing/social engineering are:

- Applying Pressure: applying emotional pressure by expressing urgency or threats to escalate to someone senior to push the staff to act.
- Evading: employing distractions, delays in answering, confusing answers and asking for questions to be repeated to wear down the staff into acting in the hackers favour.
- Risky Action: asking for a password change, MFA reset or information, which could be to gain access, or useful for further vishing attacks.

Training around the following areas is a useful starting point:
Context: Is the caller lacking context, and being vague or evasive on the call?
Action: Is the caller asking you to change passwords or MFA details?
Speaker: Does the caller sound like who they say they are?
Emotion: Does the caller use strong emotion to get you to act?

Conclusion

The 2025 UK retail cyber-attacks have underscored a critical truth: even the most recognisable and well-resourced organisations remain vulnerable to persistent, well-coordinated threat actors like Scattered Spider.

These incidents were not isolated technical failures, but rather the result of sophisticated campaigns that exploited human behaviour, identity systems, and trusted tools. The attackers demonstrated a deep understanding of how modern businesses operate, leveraging social engineering, abusing remote access software, and embedding themselves within identity infrastructure to maximise disruption and financial gain.

For the retail sector and beyond, these events must serve as a catalyst for change. Cyber resilience is no longer just a technical challenge it is a business imperative. The lessons from these recent attacks are clear: organisations must adopt phishing-resistant MFA, secure their identity and access management systems, and maintain strict oversight of remote access tools. Detection and response capabilities must be proactive, not reactive, and recovery plans must be tested and ready to deploy at a moment's notice. The basics must be relied upon too, keeping systems up to date and critical systems suitably backed up, ready to be recovered at a moment's notice.

Perhaps most importantly, businesses must invest in their people. A well-informed workforce, supported by clear processes and strong verification protocols, remains one of the most effective defences against social engineering. Cybersecurity is not just the responsibility of IT teams—it is a shared responsibility across the entire organisation.

By learning from these attacks and implementing the layered defences outlined in this guidance, organisations can significantly reduce their exposure to similar threats and build a more resilient future.

Checklist

A generic **Mitigation Checklist** is presented in Appendix 1 which can be tailored to your own organisation.

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services at preferential rates via our network of Specialist Partners.

Crisis Communications and Business Continuity - **Horizonscan**
Cyber Security Awareness Training - **Phishing Tackle**

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

Sources and Useful Links

- Scattered Spider | CISA
- NCSC statement: Incident impacting retailers - NCSC.GOV.UK
- Digital Identity Guidelines - NIST Special Publication 800-63B
- Threat Hunting Guide, UK Gov - Detecting the Unknown - A Guide to Threat Hunting
- Identifying and Mitigating Living Off the Land Techniques | Cyber.gov.au
- Incidents impacting retailers – recommendations from the NCSC - NCSC.GOV.UK

Note: Whilst UK standards and legislation are referenced in this document, other international standards and legislation should be referenced where applicable.

Additional Information

- **Cyber Security: Top 12 Tips to Protect Against Cyber Attacks**
- **Cyber Security: Respond and Recover**
- **Cyber Security: The Internet of Things**
- **Ransomware - Cyber Loss Prevention Standard**
- **Cyber Essentials - Accreditation**
- **Cyber - Respond and Recover**
- **Cyber - Incident Response Process**
- **Cyber - Homeworking Security**

To find out more, please visit Aviva Risk Management Solutions **or speak to one of our advisors.**

Email us at riskadvice@aviva.com or 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.

Appendix 1 – Mitigation Checklist

Location	
Date	
Completed by (name and signature)	

Control area	Do we as a business...	Actionable guidance	Current status
Phishing-Resistant MFA	Prioritise FIDO2/WebAuthn or PKI-based MFA?	Deploy hardware security keys (e.g., YubiKeys) or platform authenticators (e.g., Windows Hello) using FIDO2/WebAuthn. For high-risk users (admins, execs), enforce phishing-resistant MFA by default.	
	Avoid SMS and basic push-based MFA?	Disable SMS and OTP-based MFA where possible. Replace push-based MFA with number matching or biometric-based MFA to reduce MFA fatigue and push bombing risks.	
	Phase implementation based on risk?	Start with high-value targets (admins, finance, IT) and expand to all users. Use risk-based conditional access policies to enforce stronger MFA where needed.	
	Plan to deploy MFA in legacy systems?	Identify legacy apps that don't support modern MFA. Use compensating controls like VPN enforcement, jump hosts, or legacy MFA gateways (e.g., Duo for RDP).	
SSO and IdP Configurations	Regularly audit federated identity providers?	Review all configured IdPs quarterly. Validate trust relationships, metadata, and certificate expiry. Remove stale or unused IdPs.	
	Disable unused or suspicious IdPs?	Immediately disable any IdP not in active use. Investigate any IdP with unusual configuration or login patterns.	
	Monitor for unauthorised changes to authentication flows or MFA settings?	Enable logging for all IdP configuration changes. Use SIEM alerts for changes to SAML/OIDC settings, MFA policies, or conditional access rules.	

Control Area	Do we as a business...	Actionable Guidance	Current Status
Password Policies	Require minimum 16-character passwords?	Enforce long passphrases or pa (e.g., “correct-horse-battery-staple”) via policy. Educate users on creating memorable but strong passwords.	
	Avoid periodic resets unless compromise is suspected?	Follow NIST guidance: only require resets after suspected compromise. Frequent resets lead to weaker passwords and reuse.	
	Use password managers and avoid reuse across systems?	Provide enterprise password managers (e.g., 1Password, Bitwarden). Train users to generate unique passwords per system, or have IT manage this for them.	
Remote Access	Implement application control policies to block unauthorised software?	Use allowlisting tools (e.g., AppLocker, WDAC) to block unapproved RMM tools and scripts. Monitor for shadow IT.	
	Maintain a list of approved remote access tools?	Maintain an inventory of sanctioned RMM tools. Block all others at the firewall or endpoint level.	
	Require RMM access only through VPN or VDI?	Enforce RMM access via secure channels. Use VDI or jump servers with session recording and MFA.	
	Monitor logs for unexpected RMM activity?	Set up alerts for RMM tool usage outside business hours or from unusual geolocations. Correlate with user behavior analytics.	
Detection and Response	Deploy and tune EDR/XDR solutions?	Use EDR/XDR with behavioral analytics (e.g., CrowdStrike, SentinelOne). Regularly tune detection rules to reduce false positives.	
	Configure EDR tools to detect credential dumping?	Enable detections for tools like Mimikatz, LSASS access, and suspicious PowerShell. Block known TTPs (e.g., PPL bypass)	
	Set up alerts for multiple MFA prompts in short succession?	Detect MFA fatigue attacks by alerting on rapid or repeated MFA requests. Investigate anomalies identified or staff members targeted.	
	Utilise threat intelligence and threat hunting?	Subscribe to threat intel feeds (e.g., MISP, commercial TI). Conduct regular hunts for TTPs (e.g., Okta abuse, SIM swapping).	

Control Area	Do we as a business...	Actionable Guidance	Current Status
Incident Preparedness	Store backups in physically separate or cloud-isolated environments?	Use immutable cloud storage or offline backups. Ensure backups are not accessible from production networks.	
	Ensure backups are encrypted and immutable?	Encrypt backups at rest and in transit. Use WORM (Write Once Read Many) storage or backup immutability features	
	Test restoration procedures regularly?	Conduct quarterly restoration drills. Validate RTO/RPO objectives and document lessons learned.	
	Isolate critical systems and take steps to restrict lateral movement?	Use network segmentation, tiered admin models, and just-in-time access. Monitor for lateral movement indicators (e.g., Pass-the-Hash).	
User Awareness	Train staff to recognise phishing and smishing attempts?	Run simulated phishing campaigns. Teach users to verify sender domains, avoid clicking links, and report suspicious messages.	
	Train staff to recognise vishing tactics?	Educate on voice-based social engineering. Encourage verification of caller identity and escalation of suspicious calls.	
	Train staff to recognise MFA fatigue?	Explain MFA bombing tactics. Instruct users to deny unexpected prompts and report them immediately.	
	Require multi-step identity verification for helpdesk actions?	Implement callback procedures, identity verification questions, and supervisor approvals for sensitive helpdesk requests.	

Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise, and Aviva recommend that you obtain specific advice relevant to the circumstances.

19th August 2025

Version 1.1

ARMSGI3332025