Payee Verification Policy

Business Email Compromise, Phishing, Vishing and other forms of successful social engineering costs businesses millions of pounds each year in fraudulent payments. Often, a simple additional verification, such as a phone call, could prevent costly and damaging cybercrime events.

This Loss Prevention Standard has been put together to support organisations in strengthening their processes around authorising new payments to potentially fraudulent accounts.

Version: 1.1
Date: 14th November 2025

Payee Verification Policy

Introduction

Fraudulent social engineering crime, which includes phishing, vishing and business email compromise is a significant security exposure with UK consumers losing £11.4 billion to scams in the past 12 months, up £4 billion from the previous year.

Source - Cifas.

Formalising payee verification procedures can help to reduce the exposure to such attacks, and the templates provided in this Loss Prevention Standard helps organisations compile the recommended records.

Overview

This document contains the following templates:

- Payment Verification Policy Template.
- Introduction to Payee Verification Policy Email Template – a templated email to go to staff regarding the introduction of the new policy.

Completing the Payment Verification Policy Template

Purpose Section

- Explain in simple terms why this policy exists — for example "To help protect our business from invoice redirection fraud or impersonation scams."

Scope

- Include anyone who can authorise or make payments, not just the finance team.
- Mention if it also applies to subcontractors handling your finances.

Policy Statement

- Keep the language simple and practical, staff should understand exactly what to do.
- Consider including a short example such as *"If a supplier emails to say their bank details have changed, always phone your existing contact at that company (using the number already on file or their official website) before making the change."*

Responsibilities

- List names or job titles in the organisation, e.g. "Finance Manager" or "Office Administrator".
- Make clear that everyone has a part to play.
- Be aware of potential staff absences to ensure the Policy can still respond if a number of key stakeholders are away from the business.

Acceptance and Acknowledgement

- Store signed copies (physical or digital) in HR, compliance, or shared finance folders.
- Where using Microsoft 365, Google Workspace, or similar, consider setting up a simple read receipt form for evidence.

Review

- Add reminders to calendars to review the policy each year or after any security incident.

Training

- Ensure staff are trained on the procedures outlined and record this training centrally.

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.

- Cyber Security Awareness Training **Phishing Tackle**

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

Sources and Useful Links

- Phishing: Spot and report scam emails, texts, websites and... - 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

Relevant Aviva Loss Prevention Standards include:

- **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 – Example Payee Verification Policy

Document Owner	
Approval Date	
Next Review Date	
Applicable To	

Purpose

This policy sets out how [organisation name] verifies new or changed payment instructions to help prevent fraud and financial loss. It ensures that any requests to add a new payee or amend existing bank details are always confirmed verbally using contact information we already trust, not solely relying on new details provided.

Scope

This policy applies to:

- All payments made to suppliers, contractors and other third parties.
- All requests to amend existing payment details via any method (email, telephone, Microsoft Teams chat/Slack *delete as appropriate*), including bank account numbers or sort codes.
- All employees, partners and directors involved in approving, processing or instructing payments.

Policy Statement

We must never rely solely on information contained in an email, letter or message when a new payee is set up or when existing payment details are requested to be changed.

Before processing any payment to a new or amended payee, we must:

- Verify the change via a secondary contact method. Always telephone the trust contact number held on file or found on a trusted or published website.
- Do not use contact details held within the same requested instruction unless you have confirmed authenticity via the secondary source.
- Record evidence of the verification, noting the date, time and who you spoke to.
- If in doubt, DO NOT PROCEED WITH THE TRANSACTION. Take a moment and consult with a manager or finance lead to verify the transaction or change.

Responsibilities

Role	Responsibility
Finance Team/Accounts Payable	Ensure all new payee and amended payment details are verified as per this policy before processing payments. Maintain records of all checks carried out.
Managers/Directors	Ensure employees understand and follow this policy. Support staff in escalating suspicious activity.

All Employees	Follow verbal verification procedure before making or authorising any payments. Report any suspected fraudulent activity immediately.

Acceptance and Acknowledgement

All (*DELETE AS APPROPRIATE*) Partners, Senior Managers, Directors, and Employees must confirm they have read, understood and agree to comply with this policy. Confirmation can be recorded by:

- Signing below.
- Confirming acceptance via email.
- Accepting the policy through a digital HR or compliance platform.

Name……

Signature……

Date……

Policy Review

This policy will be reviewed annually or sooner if:

- Payment processes change.
- New fraud trends have emerged.
- An incident occurs that requires strengthening of this policy.

Appendix 2 – Email Template: Introduction to Payee Verification Policy

Subject: *New Policy: Verifying Payee Details to Help Prevent Payment Fraud*

Dear Team,

We're introducing a simple but important new policy to help protect our business, and our clients, from payment and invoice fraud.

Criminals are increasingly targeting UK businesses by impersonating suppliers or sending fake requests to change bank account details. These scams can look genuine using real logos, signatures, and even hacked email accounts. A single mistake can result in payments going to the wrong place and serious financial loss.

To prevent this, we've now formalised our approach in a **Payee Verification Policy**. It applies to **all Partners, Directors, and Employees** who are involved in making or authorising payments.

What You Need to Do

From now on, whenever you:

- Set up a **new payee**, or.
- Receive a **request to change existing bank details**,

you must **confirm the change verbally** using **contact details we already hold on file** or that are published on the supplier's official website.

Please **do not** rely solely on the information in the email or letter that requests the change. Hacking groups often provide fraudulent contact numbers and email addresses.

Once the verification call is made, make a brief note of:

- The date and time you called,
- Who you spoke to, and,
- Their confirmation that the details are correct.

If anything doesn't look or feel right, stop and speak to your manager or the finance team before acting.

Why This Matters

This simple step — making a quick phone call to a trusted contact — is one of the most effective ways to stop payment diversion fraud. It's a core control that insurers, banks, and regulators now expect businesses to have in place.

Next Steps

1. Please take a few minutes to read the **Payee Verification Policy** [*attach or link to document*].
2. Confirm that you've read and accepted it by [*signing the acknowledgement form / replying to this email / completing the short form here*].

3. If you have any questions or would like an example of how to verify a payee, contact [insert name or team].

Thank you for helping keep our business secure. Even small steps like this make a big difference.

14th November 2025

Version 1.1

ARMSGI3532025

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.