

Call-Back Procedure Template

Call-back controls are among the most important measures to mitigate your organisation's exposure to the risk of fraud. Done correctly, call-backs prevent your organisation experiencing financial losses, even in cases where cyber-criminals have managed to deceive your Accounts Payable team into manipulating supplier banking information.

So, it's critical you do call-backs right.

This 5-step checklist is designed to ensure you meet industry best-practice when it comes to call-back controls.

Control Activity	Control Process
1 Independently Source Phone Number	<p>NEVER use phone numbers sourced from the body of an email or from an invoice that has been sent via email.</p> <p>NEVER click a link to a supplier's website contained in the body of an email or from an invoice that has been sent via email.</p> <p>ALWAYS source supplier contact information from the supplier's official website by opening a new web-browser and manually typing in the supplier's domain name.</p>
2 Multiple Verifications of Phone Number	<p>ALWAYS verify the accuracy of supplier contact information across five (5) independent sources:</p> <ul style="list-style-type: none">• Supplier website• White Pages / Yellow Pages• Official Social Media Profiles, e.g. LinkedIn• Google the supplier name to verify whether the same contact information is listed across multiple separate websites, e.g. Government sites, industry listings sites, local community sites, etc.
3 Initiate Calls via Outbound Line	<p>NEVER rely on any inbound calls to verify supplier banking information. Even if the inbound call looks to be from a legitimate/known number, such calls may have been spoofed.</p> <p>ALWAYS initiate outbound calls when verifying supplier banking information.</p>
4 Verify Identity of Authorised Third-Party	<p>ALWAYS call a supplier's switchboard and ask to be directed to the Accounts Payable department.</p> <p>ALWAYS note the name and position of the individual with whom you are verifying supplier banking data.</p> <p>ALWAYS ensure the individual is a representative of the legitimate supplier by asking questions ONLY a representative of a legitimate supplier should have answers to, such as:</p> <ul style="list-style-type: none">• Value of last three (3) invoices paid by your organisation to the supplier• Date of initial invoice that your organisation received from the supplier• Purchase Order (PO) number of initial order that your organisation placed with the supplier
5 Verify Validity of Bank Account Information	<p>ALWAYS ask for permission to record calls confirming Account Name, BSB and Account Number.</p> <p>ALWAYS ask to be sent a PDF of the header of the supplier's bank statement, showing the Account Name, BSB and Account Number.</p>

Following each of the 5 steps in this call-back checklist will significantly mitigate your organisation's risk of experiencing a serious fraud incident.

For further advice on securing your payments processes, contact eftsure: get.eftsure.com.au