ALL CALL-BACK PROCEDURES ARE NOT THE SAME

PREPARED BY
DENNIS GUSTAFSON

AHT INSURANCE
A BALDWIN RISK PARTNER

ALL CALL-BACK PROCEDURES ARE NOT THE SAME

We are seeing more and more Funds Transfer and Social Engineering (aka Impersonation Fraud) claims and coverage for these claim scenarios vary from carrier to carrier. There are several differentiating factors that could cause one carrier to approve a claim and another to deny, but the most common is how they structure their call-back requirements.

Just in the past year, we saw nine different carriers respond to similar funds transfer claim scenarios. When we saw challenges to a claim, they were almost always based on a perceived failure by the bank to meet the listed call-back requirement. As we compare all nine, here are several key differences that should be reviewed prior to the next claim.

Social Engineering versus Funds Transfer Fraud: As many Fidelity Bond policies offer the Social Engineering coverage with a sub-limit versus the full Funds Transfer Fraud limit, it is helpful to determine early on, during the investigation of the loss, how it will be categorized. The easiest way to contrast is that Social Engineering (SE) usually relates to the loss or theft of the entity's own funds whereas Funds Transfer Fraud usually relates to the loss or theft of a customer's funds. While we have seen Social Engineering sub-limits as low as $50,000, the most common sub-limits are $250,000, $500,000 or $1,000,000. They are often based on the overall limits (i.e., a $10M Bond is much more likely to have a $1M SE sub-limit than a $2M Bond)

- **When is a call back required?** There is usually a dollar threshold whereby all transfers greater than that dollar amount require some form of call-back. The larger the threshold, the better. The most common threshold matches the Bond deducible, otherwise, they usually range between $25,000 - $50,000.

- **What are the ranges of call-back requirements** from perceived least to most restrictive?
  - No call-back requirements: For some cyber policies, which may extend to covering Funds Transfer Frauds or other Social Engineering coverage grants, there are no call-back requirements. While this does exist, we would say it is available less and less as we see more claims.

  - Underwriting approved: Some bond policies include generic language that states any call-back type can be accepted, as long as that type of verification was first approved by an underwriter. If your policy includes that, we suggest you coordinate a call with the Bond underwriter to share the Bank's current call-back process/procedure for their confirmation of acceptance.

  - Simple call back: Sometimes the only requirement is a confirmed call back to a pre-determined number.

  - **Or** is always better than **and**: One carrier states that acceptable call-back verification can be done by a valid test key ***or*** a call-back to the person who initiated the instructions ***or*** digital signature or use of username and password/pin or biometric authentication or any other recognized two-factor e-authentication.

AHT INSURANCE
A BALDWIN RISK PARTNER

ALL CALL-BACK PROCEDURES ARE NOT THE SAME

Only One Type of Call Back is Acceptable:

- Only acceptable call back is the existence of some form of valid test key, which has been mutually agreed upon by the customer and the insured.
- Some form of out-of-band (median difference from original request) verification (voice, email, text) to a pre-determined location requiring an affirmative reply.
- One carrier states that commercial customer coverage only applies if the transmittal method by which the Institution received the Fraudulent Transfer request matched the authorized method.

More stringent is the existence of multiple requirements:

- Requirement of Out-of-Band verification ***and*** it must be recorded for coverage to be afforded.
- Two-Factor Authentication (typically representing some form of user ID, PIN, Token or Dual Authorization) ***and*** the existence of a Written Agreement.
- Call Bank to the predetermined number set forth in the written agreement ***and*** the Institution preserved a recording of the call back/verification.
- Sender verified instruction with a password, PIN, or code and call back to the pre-determined telephone number (documented in the written agreement), ***and*** verification preserved.

Most stringent requirements: And lastly, the requirement that is perceived to be the highest hurdle to get over is the requirement of some type of handwritten signature verification from two separate employees (within their authority). Note: this level of stringent requirement often goes hand-in-hand with a much greater Social Engineering limit including up to the full limit.

In summary, we see significant variations to call-back requirements and, as such, we recommend reviewing what policy language is in place prior to any claim scenario to give the institution as good a chance as possible to realize claims coverage.

AHT INSURANCE
A BALDWIN RISK PARTNER