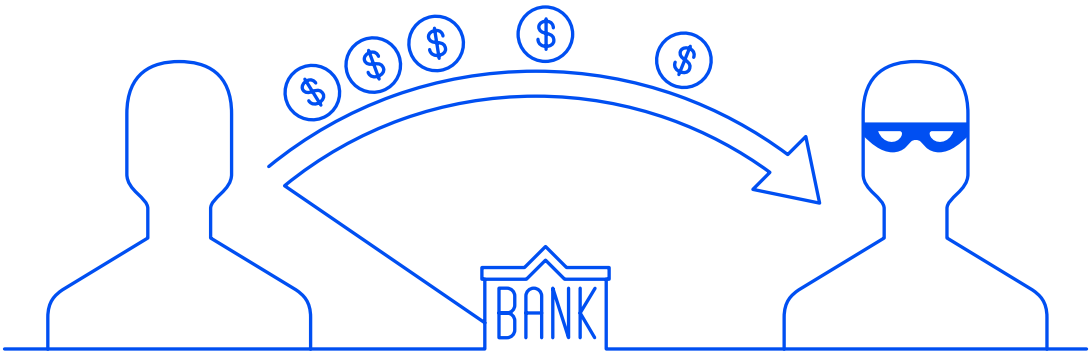
Funds Transfer Loss Authentication Endorsement

What is Funds Transfer Fraud?

Funds Transfer Fraud involves a variety of deceptive schemes whereby a threat actor convinces an unsuspecting victim to transfer funds to another party under fraudulent circumstances. Threat actors exploit trust and complacency to manipulate victims into transferring funds electronically leading to financial losses.



What is a Funds Transfer Loss Authentication Endorsement?

A funds transfer loss authentication endorsement is an amendment to an insurance policy designed to mitigate losses incurred through the unauthorized or fraudulent transfer of funds. The endorsement requires the policyholder to implement and maintain a secondary means of authentication to verify bank account coordinates when initiating a payment to new customers, as well as verifying requests to change the bank account coordinates of existing customers.

Threat actors exploit trust and complacency to manipulate victims into transferring funds electronically leading to financial losses.

How does a Funds Transfer Loss Authentication Endorsement Apply?

The endorsement requires the policyholder to verify, through a secondary means, bank account coordinates of new accounts, and when processing changes to an existing account.

> *Example:*
> *You're expecting an invoice via email from a vendor. You receive what appears to be a legitimate invoice, but it includes a note advising that the bank account coordinates have changed. For coverage to apply, the endorsement requires that the change be verified through a secondary means. A phone call to a trusted person on the receiver's end would satisfy the requirement.*

Why is it important to verify customer bank account information and why does my insurer require it?

As a condition of the policy, it's important to authenticate customer bank account information to ensure a claim involving funds transfer fraud is paid. Requiring verification is a preventative measure that helps to ensure the legitimacy of the receivers account information and reduces the likelihood of fraud, thereby enhancing your security posture and reducing the probability of experiencing a funds transfer fraud claim.

Examples of Secondary Authentication Methods:

Phone call to a trusted person on the receiver's end

Don't be a Victim:

- Be suspicious of any request to change bank coordinates.
- Scrutinize the email address from where the change instructions were sent.
  - While the email address may look legitimate at first glance, often it will be modified slightly to appear legitimate.
- Implement multi-factor authentication (MFA) on email accounts.
- Provide cyber awareness education to your employees
- Test your employees cyber awareness through simulated phishing exercises using tools that mimic real-world threats
  - Create scenarios with phishing emails or messages that gauge their responses
  - Monitor who fails and provide targeted training to reinforce awareness
  - Regularly update tests to stay ahead of evolving cyber threats