CORY WASHINGTON & CO.

SMARTER RISK. STRONGER BUSINESS.

CWCO-SUP-CRIME-CHK Rev. 09-2026

COMMERCIAL CRIME — POLICY FEATURE CHECKLIST

Pull out your current crime policy and check the box next to each feature you can confirm it includes — anything unchecked is worth a quick conversation with your advisor.

STANDARD **OFTEN LIMITED** **IF NEEDED** *— Standard: should be included · Often limited: frequently sublimited, excluded, or optional · If needed: depends on your operations*

	POLICY FEATURE	WHAT TO CONFIRM	PRIORITY
☐	**Employee Theft**	Covers money, securities, and property stolen by employees — the core of the policy.	STANDARD
☐	**Social Engineering**	Covers payments sent after fake emails or calls — usually a small sublimit or excluded.	OFTEN LIMITED
☐	**Funds Transfer & Computer Fraud**	Covers theft by unauthorized transfers or system manipulation.	STANDARD
☐	**Forgery or Alteration**	Covers forged or altered checks and payment instructions.	OFTEN LIMITED
☐	**Money & Securities (Inside and In Transit)**	Covers robbery, burglary, and theft of cash on premises and on the way to the bank.	OFTEN LIMITED
☐	**Client Property (Third-Party)**	Covers theft by your employees from clients — often required by client contracts.	IF NEEDED
☐	**ERISA Fidelity Bond**	Required by law for retirement plans — at least 10% of plan assets, usually up to $500,000.	IF NEEDED

COMMON GAP IN THIS COVERAGE

The most commonly missed gap in this coverage is social engineering. Many crime policies cover theft by employees but exclude, or sharply sublimit, money sent to fraudsters after fake emails — while small businesses have the highest median fraud losses and a typical scheme runs a year before detection. Businesses should confirm the social engineering limit and separate who sets up vendors from who pays them.

IMPORTANT — PLEASE READ