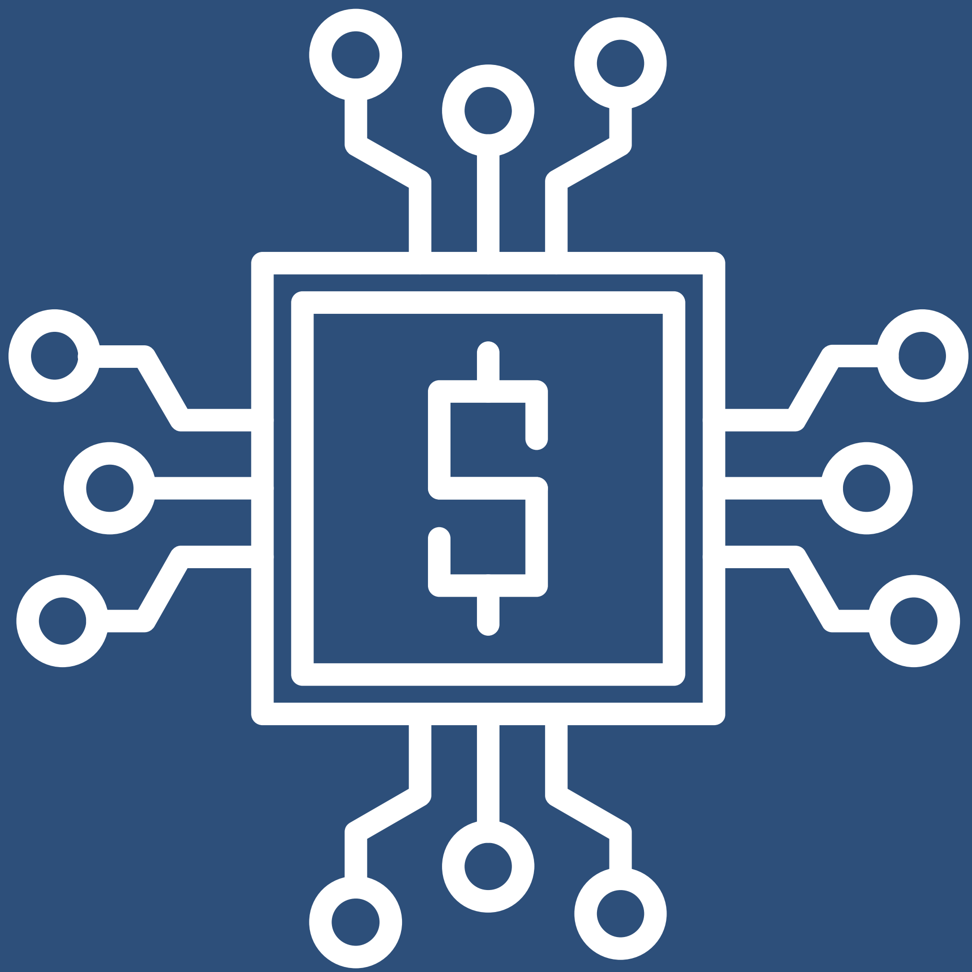
Continuum



Fintech Fraud Where Cyber Stops and Crime Begins

Three fraud types. Two policies. One question: which one covers yours?

Continuum

Cyber: Breach Response and Business Interruption

Cyber covers losses arising from security incidents and data breaches.

- **Breach response, forensic investigation, and notification costs**
- **Business interruption from the security failure**
- **System recovery and remediation**

Responds when a breach causes the loss.

Continuum

Crime: Employee Dishonesty

Crime covers employee theft, embezzlement, and internal fraud schemes.

- **Employee dishonesty and theft of assets**
- **Forgery and unauthorized access by staff**
- **Direct loss of money or securities**

Responds when an employee perpetrates the theft.

Continuum

Social Engineering: Crime Coverage

Customer receives a deceptive message and voluntarily transfers funds.

Voluntary transfer triggered by deception

Falls under Crime insurance, not Cyber

Different trigger, different policy

This one belongs to Crime, not Cyber.

Continuum

Funds Transfer Fraud: Account Takeover

A customer's account is compromised. Fraudsters issue unauthorized payment instructions.

- **Account takeover often carved out of standard Crime**
- **Requires specific endorsement to be covered**
- **Needs explicit coverage language in your policy**

This exposure typically needs its own endorsement.

Continuum

Vendor Compromise: Third-Party Impersonation

A payment partner is impersonated. Fraudsters request fund transfers.

- **Third-party impersonation sits outside standard coverage**
- **Requires independent verification controls to prevent**
- **Often completely uninsured unless specifically addressed**

Policy language determines whether coverage applies.

Continuum

Know Where Your Coverage Sits

Three different policies. Three different triggers. Understanding where each applies prevents coverage surprises.

Continuum helps fintech providers understand where Cyber stops and Crime begins

www.continuuminsure.com