Employee Benefit Plan Fiduciary Dishonesty Policy

And Extended Crime Endorsement

CHUBB®

Are Your Benefit Plan Assets Secured?

The Employee Retirement Income Security Act of 1974 (ERISA) requires that most employee benefit plans purchase a bond that protects against fraud or dishonest acts of its plan officials.

With a Fiduciary Dishonesty policy from Chubb, Plan Administrators and Trustees can have peace of mind that their plans are secure from loss caused by dishonest plan officials, as well as hackers, impersonators and other criminal third parties.

Policy Form Benefits

- Coverage for fraud or dishonest acts of all natural person plan officials, as required by ERISA, with no exclusion for outside independent contractors
- Pure Discovery form with no prior acts exclusion
- Minimal exclusions applicable to Fiduciary Dishonesty coverage
- Industry-leading optional coverage for loss caused by outside criminals, including:
  - Forgery of a plan's financial instruments
  - Funds Transfer Fraud from a plan's bank account
  - Computer Fraud
  - Social Engineering Fraud
  - Investigative Expenses
  - $10,000 in recovery legal costs to pursue funds from perpetrators
- Discounted two and three year prepaid premiums are available, subject to underwriting
- Coverage is available for all types of ERISA regulated plans, including: single employer, multi-employer and multiple employer arrangements, whether sponsored by private, publically-traded, not for profit or labor union under collective bargaining agreement.
- Policy can be tailored to cover government sponsored plans and other plans not subject to ERISA

Limits Available

Coverage from Chubb provides a guaranteed limit per plan in accordance with ERISA law up to:

- $25,000,000 per occurrence, with no aggregate limit.
  - Pay Over clause allows limit beyond the statute to apply to all plans; coverage is not limited to the statutory provision.
- Inflation guard provision ensures the limit will always meet minimum requirements under ERISA.

Why Chubb?

As the largest writer of Crime and Fidelity coverage in North America according to the Surety and Fidelity Association of America, Chubb is particularly situated to understand and underwrite the bonding coverage required for multi-employer, multiple and single employer plans, hav ing provided coverage for such plans since 1974.

Fiduciary Dishonesty Coverage

Providing coverage beyond just meeting a regulatory requirement, Chubb's Fiduciary Dishonesty policy provides administrators and trustees with the ability to cover all plan officials who need to be bonded, not just those employed by the plan.

Loss Scenario: Third Party Administrator Runs Amok

A local labor union hired an outside third party administrator to manage their retirement and welfare benefit plan contributions, payment of claims to beneficiaries and the maintenance of bank accounts. Over a period of five years, the administrator transferred benefit funds to accounts he controlled and freely spent the funds on non-union expenses. The administrator also charged the union for expensive computer consulting and office equipment which either never arrived or was unnecessary. Finally, the administrator established multiple fraudulent programs designed for no other reason other than to funnel payments to an affiliated company owned by the administrator.

Resolution: Crippled under the weight of increasing theft and mounting negative account balances, the administrator resigned, triggering an investigation by auditors. It was revealed that the administrator had unchecked access to bank accounts, authority to spend the fund's money without oversight from the trustees, and a voracious appetite for expensive goods and services. Prior to being caught, the administrator had embezzled more than $10 million through a number of different methods, including fabricated invoices, direct withdrawal from fund accounts, and fraudulent expenses over a period of five years.

Social Engineering Fraud Coverage

Unique and innovative, Chubb's Social Engineering Fraud coverage for Employee Benefit Plans addresses impersonation of the following parties:

- Administrators
- Trustees
- Employees of Vendors
- Employee Benefit Plan Participants

Loss Scenario: Beneficiary or Imposter?

As part of a multi-employer defined contribution plan offered by a local union, employees were given online access to their account, allowing them the ability to update their address, contact information and beneficiary information. The plan provided each participant with a unique login and required a unique password to gain access to the system, and in the event of changes to the system required a secondary verification before processing the change. A plan participant called the pension administrator's office to complain that they could not access their account. When the administrator reviewed their account, it was virtually empty having been transferred to an unknown IRA account.

Resolution: After an investigation, it was determined that the participant's password and user name had been compromised through a phishing scheme, wherein a criminal pretended to be the benefits administrator and "requested" the user input their information into a form which allowed them access to the system as if they were the plan participant. The criminal changed all contact information and bank account routing information to an account they controlled. Upon requesting the controlled account be transferred, the fraudsters correctly responded to the required verification questions and phone calls using the information harvested during the phishing campaign and successfully stole nearly $500,000 from the plan participant.

Funds Transfer Fraud Coverage

With the rise of online banking, benefit plans are increasing exposed to theft of banking credentials which allows perpetrators to convince a bank to transfer money under the guise of a legitimate plan representative.

Loss Scenario: Bank Account Hijacked

A fund employee was reviewing a report of Automated Clearing House wire transfers made on the fund's bank account during the last week. The report showed six unusual postings. The employee contacted the bank and was informed that the payments had been made from the fund's access to their online portal, and from their perspective were in fact authorized.

Resolution: After an investigation, it was determined that the employee's computer had been compromised with malware, and a key logging program had captured the user name and password of the employee, allowing an outsider to gain access and transfer the funds by communicating directly with the bank. Six transfers had been processed, totaling $125,000, but more importantly 50 others were set to automatically transfer over the next few days totaling millions which luckily were stopped.

How Do I Get a Quote?

Contact your local agent or broker today and request an application. Short form applications are available for plans requesting limits of $1,000,000 or less.

Chubb appointed agents and brokers can send new business submissions to NBSEmails@chubb.com and will receive direct service and support from a team of specialized underwriters.

Contact Us

For more information on Chubb's Fiduciary Dishonesty policy and Extended Crime Endorsements, contact:

Chris Arehart
Senior Vice President
carehart@chubb.com
312-529-6700
www.chubb.com/us/crime

Chubb. Insured.℠