

Plastic Card Protector Insurance Policy



Insurance | Risk Management | Consulting



The Gallagher Plastic Card Protector Insurance Policy is an innovative and modern approach to protecting card issuers against fraudulent losses, whether these losses are caused by traditional card fraud techniques or by new and sophisticated cyber threats. The policy is designed to safeguard margin losses and provide profit protection by responding to losses above expected tolerances.

The Need for Coverage

Card fraud is on the rise and cardholder details are increasingly vulnerable to the data breaches experienced by major retailers and financial institutions. Cardholder details are being sold on the “dark web” where they have become a criminal commodity sold to the highest bidder. The potential losses caused by the mass sale of stolen data are at a level previously unseen and expose card issuers to substantial peaks in excess of their known attritional loss levels.

Traditional forms of plastic card fraud remain ever present with total fraud losses increasing year on year since 2010.

Despite the high incidence of plastic card losses and evidence that the trend is growing, protection by insurance is often overlooked. Crime policies seldom provide coverage for such losses. Most policies include a specific plastic card exclusion and even if such exclusion is not present, affirmative coverage is rarely provided. Many plastic card insurance policies fail to deal with modern cyber threats, providing cover solely for the risk of physical card fraud.

The Gallagher Plastic Card Protector Insurance Policy covers this shortfall in protection.

What Does This Cover?

It covers lost, stolen, counterfeited or compromised credit cards, debit cards, ATM cards, digital representations of such cards and the card identification theft.

The main areas of coverage are for the unauthorized use of lost, stolen and counterfeit cards, unauthorized use of card identification data, and the use of a PIN without authority.



How Can Losses Arise?

- Fraudulent use of card identification data to generate fictitious transactions
- Fraudulent use of a card at an electronic terminal
- Fraudulent use of a card via telephone, mobile device, the internet and other similar modes of communication
- The incurring costs of reissuing compromised cards

General Policy Provisions

The insurer is only entitled to exercise its rights for nondisclosure, misrepresentation and breach of warranty in the event of fraud.

- Extended reporting period options
- Clear reporting provisions

The information contained herein is offered as insurance industry guidance and provided as an overview of current market risks and available coverages and is intended for discussion purposes only. This publication is not intended to offer legal advice or client-specific risk management advice. Any description of insurance coverages is not meant to interpret specific coverages that your company may already have in place or that may be generally available. General insurance descriptions contained herein do not include complete insurance policy definitions, terms, and/or conditions, and should not be relied on for coverage interpretation. Actual insurance policies must always be consulted for full coverage details and analysis.

Insurance brokerage and related services to be provided by Arthur J. Gallagher Risk Management Services, Inc. (License No. OD69293) and/or its affiliate Arthur J. Gallagher & Co. Insurance Brokers of California, Inc. (License No. 0726293).

Example Scenarios

- A card issuer sends out new, replacement, renewal or additional cards to cardholders. The cards are stolen prior to being delivered and are then sold nationally or worldwide to obtain cash advances through other financial institutions or are used to make unauthorized purchases.
- A major retailer is the victim of a significant hack. As a result, thousands of cardholder details are obtained by the hackers who then post them for sale on the dark web. The details are subsequently obtained by a criminal network that systematically exploits the details to make unauthorized transactions, resulting in huge losses.
- Cards are counterfeited by skimming. The counterfeit cards are then used to make unauthorized purchases and cash withdrawals.
- A card is printed, embossed or encoded with a cardholder's account number, and used without permission in a "card present" environment through a key entered, rather than a swiped procedure.

For more information, contact Eileen Yuen, U.S. managing director of Gallagher's Financial Institutions practice at eileen_yuen@ajg.com or 973.921.8283 or Murray Farquharson, U.K. Divisional Director of Gallagher's Financial Institutions Practice at murray_farquharson@ajg.com or +44 (0) 20.3425.3146.



The Gallagher Way.
Since 1927.

ajg.com