TOKIO MARINE HCC

NetGuard® SELECT

CLAIMS EXAMPLES

Our insureds say it best: "Trusted, responsive, and there when it matters most."

Claims examples are a great way to bring cyber coverage to life, showing how policies respond when it really matters. They help clients understand risks in a relatable way and see the true value of having the right protection in place.
Here are some examples:

01. CYBER CRIME COVERAGE– CRYPTOCURRENCY PHISHING

The insured received an unsolicited call from someone posing as a technical support specialist from a cryptocurrency exchange he frequently used. The caller claimed the insured's account had been frozen and requested his username and password to reactivate it. Believing the call to be legitimate, the insured provided his credentials. Shortly thereafter, the fraudster converted the insured's various cryptocurrency holdings into Ethereum and withdrew the funds from his account.

Upon discovering the unauthorized activity, the insured notified Tokio Marine HCC (TMHCC) under his personal cyber policy. TMHCC's Cyber Claims team walked the insured through immediate containment steps and coordinated with the exchange and relevant financial institutions to attempt fund recovery. Despite those efforts, the stolen cryptocurrency could not be retrieved.

Cyber Crime Coverage under the personal cyber policy responded to the unrecoverable loss. The policy paid $64,329 to reimburse the insured for the stolen cryptocurrency, subject to applicable terms and conditions.

This case illustrates how personal cyber insurance can help individuals recover from sophisticated phishing schemes, turning what would have been a total crypto currency loss into a manageable incident and restoring financial stability after a high-impact cybercrime event.

02. CYBER CRIME COVERAGE – PERSONAL BANK ACCOUNT WIRE TRANSFER FRAUD

> The two initial wire transfers totaling $160,000 had already been processed and could not be reversed.

An unknown individual gained access to the insured's personal bank account and initiated four unauthorized wire transfers. Around the same time, the insured began receiving multiple spam emails and spoofed text messages that appeared to be from her bank. These messages stated that charges were being processed and requested confirmation to proceed. Relying on these communications, the insured initially approved two of the transfers before becoming suspicious and denying the remaining two.

Later, the insured received legitimate communication from her bank indicating that someone had logged into her account from an unrecognized device. At that point, she realized her account had been compromised and reported the incident. However, the two initial wire transfers totaling $160,000 had already been processed and could not be reversed.

The insured reported the loss to TMHCC under her personal cyber policy. TMHCC's Cyber Claims team promptly engaged with the insured and her bank, confirmed the scope of the fraud, and provided guidance on securing her account and devices against further compromise. Cyber Crime Coverage under the policy responded, by reimbursing the insured for a portion of the unrecoverable funds. The coverage also paid the costs of hiring a technology consultant to remediate the compromised devices and enhance security going forward.

This incident demonstrates how personal cyber coverage can significantly mitigate the financial impact of account takeover fraud, while also providing expert support to help insureds secure their finances and digital lives after an attack.

03. CYBER CRIME COVERAGE – ACCOUNT TAKEOVER OF A HIGH-PROFILE INDIVIDUAL

The General Manager of a prominent sports franchise noticed suspicious activity in his personal bank accounts and found himself unable to access his primary email account. At the same time, his family members began receiving unusual text messages and phone calls appearing to originate from his phone number. Concerned about the breadth of the compromise, the insured contacted his personal cyber claims team at Tokio Marine HCC (TMHCC) for assistance.

Immediately upon notice, TMHCC's Cyber Incident Management team activated a coordinated response, recommending the retention of breach counsel and a leading forensic investigation firm to take swift action. A scoping call was held without delay to assess the scope of the compromise, prioritize containment steps, and protect both the insured and his family.

The investigation revealed that the threat actor had used multiple data broker websites to gather personal information about the insured and his family. Armed with this data, the attacker correctly answered security questions to gain access to the insured's primary email account and initiate fraudulent banking activity. Working with law enforcement and banking contacts, TMHCC helped reverse the majority of the fraudulent transactions and secure the insured's accounts and devices.

This case underscores how personal cyber insurance can be especially critical for high-profile individuals and families, providing rapid access to cyber experts, law enforcement coordination, and financial protection when targeted by sophisticated threat actors.

The investigation revealed that the threat actor had used multiple data broker websites to gather personal information about the insured and his family.

04. CYBER EXTORTION COVERAGE – MOBILE DEVICE CONTENT THREAT

The insured received a prompt on his mobile device requesting that he enter his Apple ID and password to access an application. Believing it to be a normal authentication request, he entered his credentials. About a week later, the insured was contacted by an individual claiming to be a hacker who alleged that he had downloaded the insured's phone contents, including sensitive personal photos, and demanded payment of two Bitcoin (approximately $206,000 at the time) to avoid releasing the images publicly. The insured immediately reported the threat to Tokio Marine HCC (TMHCC) under his personal cyber policy and triggered the cyber extortion coverage. TMHCC's Cyber Incident Management team activated a coordinated response, recommending the retention of breach counsel, a forensic investigation firm, and arranging a scoping call to quickly assess the credibility of the threat and the extent of any compromise.

Working closely with law enforcement and forensic experts, TMHCC helped trace the threat actor's activity and evaluate whether the attacker had genuine access to the insured's data. Based on the findings and risk assessment, TMHCC negotiated a reduced, partial ransom payment to mitigate the cyber extortion threat, while also guiding the insured through measures to secure his Apple ID, devices, and cloud accounts.

The personal cyber policy's Cyber Extortion Coverage responded to:

- The negotiated ransom payment where the attacker agreed not to release stolen data from the insured's personal device.
- Forensic and legal fees associated with validating the threat and coordinating the response.
- Ongoing security support to help the insured harden his personal accounts against future attacks.

This incident highlights how personal cyber insurance can provide both financial protection and expert negotiation support in emotionally charged extortion scenarios, helping individuals navigate complex threats they would struggle to manage alone.

05. CYBER EXTORTION – FAKE WEBCAM COMPROMISE

The insured received an alarming email that appeared to come from his own email address. The sender claimed to have compromised the insured's webcam, recorded sensitive images and videos, and threatened to send the content to all of the insured's contacts, including friends and family, unless a ransom was paid. The email referenced the insured's email password and contact list to lend credibility to the threat.

The insured promptly reported the incident to Tokio Marine HCC (TMHCC) under his personal cyber policy and triggered the cyber extortion coverage. TMHCC's Cyber Incident Management team quickly activated a coordinated response, retaining breach counsel and a forensic investigation firm and arranging a scoping call to evaluate the validity of the extortion demand and determine whether any accounts or devices had actually been compromised.

> TMHCC advised the insured not to engage with the threat actor or make any payment, and guided him through steps to reset credentials and enable stronger security settings across his accounts.

Through forensic analysis and review of the email headers, TMHCC and its experts determined that the extortion message was part of a widespread scam campaign, and that there was no evidence of actual webcam access or device compromise. With this confirmation, TMHCC advised the insured not to engage with the threat actor or make any payment, and guided him through steps to reset credentials and enable stronger security settings across his accounts.

Although no ransom payment or direct loss ultimately occurred, the personal cyber policy provided valuable benefits by:

- Providing legal and advisory support to ensure appropriate handling of the incident.
- Giving the insured confidence and peace of mind that his privacy and accounts remained secure.

This case demonstrates that personal cyber insurance is not only about reimbursing losses; it also offers insureds access to trusted experts who can quickly assess threatening situations, prevent unnecessary payments, and help them respond calmly and effectively.