

# Cyber Claims Scenarios for Financial Institutions

Here are examples of recent claims scenarios to give you a sense for our capabilities:

## Phishing Scam

*More than 400 employee e-mail accounts were compromised in an e-mail phishing attack.*

<b>Industry</b>	Financial Institutions
<b>Business</b>	Commercial
<b>Claims Difference</b>	Top-Tier Response Coach and Forensic Firm
<b>Description</b>	A financial institution recently became the victim of an e-mail phishing attack targeted against its employees. As a result of the attack, more than 400 employee e-mail accounts were compromised. The financial institution retained a forensic firm to investigate the extent of the breach, as well as an incident response coach from the Chubb Cyber Panel. Data mining and a review of what information was compromised is ongoing. This initial phase of the incident response will cost more than \$1.5M for both the coach and forensic firm. Once this review is complete, there will be an assessment as to whether notification and credit monitoring services are necessary.

## Ryuk Ransomware

*Ryuk is a virulent form of ransomware that is characterized by large ransom demands.*

<b>Industry</b>	Financial Institutions
<b>Business</b>	Commercial
<b>Claims Difference</b>	Superior Coverage
<b>Description</b>	A financial institution was the victim of a Ryuk ransomware attack. Ryuk is a virulent form of ransomware that is characterized by large ransom demands. This type of attack is usually preceded by a type of malware, called a banking “Trojan,” which enables the bad actor to view its victim’s internal financial information. In this particular attack, the ransom demand was for more than \$1M in Bitcoin, which the company refused to pay. This attack, like most ransomware attacks, rendered the company’s data inaccessible. An incident response coach and a forensic firm from Chubb’s Cyber Panel were retained in accordance with the Network Extortion Insuring Agreement under the Chubb Cyber Policy. Although the company has recovered by utilizing the backups to its system, the forensic firm is still determining the extent of any potential damage the insured may have sustained and if any remediation is necessary. These firms are also determining if protected information was compromised in a manner that would trigger notification obligations under applicable data privacy laws.

### ATM Skimming

*More than 400 bank customers had their information stolen from an ATM card skimmer.*

<b>Industry</b>	Financial Institutions
<b>Business</b>	Commercial
<b>Claims Difference</b>	Expert Claims Investigation
<b>Description</b>	The insured financial institution discovered that a bad actor installed a card skimmer at one of its drive-up ATM machines. The skimmer was not detected for several days and more than 400 bank customers had their information stolen. Several fraudulent banking transactions were processed as a result of this incident. The relevant Crime Policy came into play, and Chubb was also notified of the incident under the Chubb Cyber Policy. An incident response coach was retained from Chubb’s Cyber Panel under the Incident Response Fund Insuring Agreement of the Cyber Policy. The affected individuals were notified and provided with credit monitoring services through one of Chubb’s panel notification firms. Chubb continues to monitor for third party suits from the affected customers.

### Rogue Employee

*A rogue employee used several newly issued credit cards for their own personal use.*

<b>Industry</b>	Financial Institutions
<b>Business</b>	Commercial
<b>Claims Difference</b>	Technical Expertise
<b>Description</b>	An employee of a financial institution had access to new credit cards that were being issued to its customers. Over a period of several months, this rogue employee used several of these credit card numbers for their own personal use. The employee was eventually caught and arrested. The insured retained counsel from the Chubb Cyber Panel. Counsel is in the process of determining whether there are any notification obligations by the institution, as well as whether credit monitoring services should be offered to the card holders. Counsel is prepared to defend the insured against any third party suits that may be brought by affected individuals as a result of the mishandling of their credit card information.

## Ready to sell Chubb?

Visit our website for more information about Chubb’s insurance solutions.

The claim scenarios described here are intended to show the types of situations that may result in claims. These scenarios should not be compared to any other claim. Whether or to what extent a particular loss is covered depends on the facts and circumstances of the loss, the terms and conditions of the policy as issued and applicable law.

Chubb is the marketing name used to refer to subsidiaries of Chubb Limited providing insurance and related services. For a list of these subsidiaries, please visit our website at [www.chubb.com](http://www.chubb.com). Insurance provided by Chubb Insurance Company of Canada or Chubb Life Insurance Company of Canada (collectively, "Chubb Canada"). Risks subject to full underwriting review and acceptance; premiums may vary. Reasons listed for why an insured chose Chubb based on perceptions of Chubb employees from communications with producers. All products may not be available in all provinces or territories. This communication contains product summaries only. Coverage is subject to the language of the policies as actually issued. Chubb Canada, Suite 2500, 199 Bay Street, Toronto ON M5L 1E2.