

Crime Loss Response Checklist



Steps to Take After a Crime

A crime-related loss can be disruptive and costly, but a structured response can help mitigate damage and protect your business. Whether it's theft, fraud, vandalism, or cybercrime, taking immediate action ensures safety, preserves evidence, and facilitates a smooth claims process. This checklist provides key steps to follow after a crime-related loss.

1. ENSURE SAFETY AND SECURE THE SCENE

- **Ensure the safety of individuals:** Make sure employees, customers, and other individuals are safe and away from the scene if there is any immediate danger.
- **Call law enforcement:** Report the crime to local authorities and request a police investigation. If the crime is ongoing (e.g., a break-in), ensure that you alert law enforcement immediately.
- **Secure the premises:** If possible, prevent further unauthorized access. Lock doors, close windows, and secure entry points to avoid further loss or damage.

2. NOTIFY KEY INTERNAL STAKEHOLDERS

- **Alert management and senior personnel:** Notify relevant internal stakeholders, including executives, legal, and risk management teams, of the incident.
- **Involve HR and security:** Ensure that Human Resources (HR) and security teams are aware of the situation if employee misconduct or a security breach is involved.

3. DOCUMENT THE INCIDENT

- **Record initial details:** Take notes of what has been stolen, damaged, or affected, including the time, date, and nature of the crime.
- **Take photographs or videos:** Document the scene with photos or videos for evidence. This can include damage, items that are missing, or any signs of forced entry.
- **Preserve evidence:** Do not disturb the crime scene until law enforcement has arrived, if applicable. Any physical evidence may be crucial for the investigation.

4. CONTACT GRANITE INSURANCE AGENCY ASAP

- **Report the loss to your insurance agent:** Notify your insurance agent about the crime loss as soon as possible. Provide them with a detailed account of the incident and any initial damage estimates.
- **Understand your coverage:** Review the insurance policy with your assigned claims adjuster and your agent to understand what is covered, the deductible, and the claims process.
- **Request a claims adjuster:** Ask the claims adjuster to assess the damage, stolen property, or loss of business.

5. NOTIFY LEGAL COUNSEL

- **Consult with legal advisors:** Depending on the nature of the crime (e.g., employee theft, fraud, or data breach), consult with legal counsel to ensure compliance with relevant laws and to assess potential legal implications.
- **Determine reporting obligations:** Identify if you are required to notify regulatory bodies (e.g., in cases of identity theft, financial fraud, or breach of customer data).

6. SECURE DIGITAL ASSETS AND DATA

- **Notify IT team (if relevant):** If the crime involves data theft, hacking, or other digital crimes, inform your IT department immediately.
- **Review system logs:** Work with IT to identify if any data was accessed, stolen, or compromised, and assess potential exposure to sensitive or personally identifiable information (PII).
- **Change passwords and access credentials:** Change access passwords for critical systems, especially if the crime involves an internal threat or compromised systems.

7. IDENTIFY AND ISOLATE AFFECTED AREAS

- **Isolate affected areas:** If the crime involved damage to property or equipment, isolate the affected areas to prevent further harm or contamination (e.g., securing computers or physical assets).
- **Investigate the scope of loss:** Identify all items, data, or resources affected, and create an inventory of missing or damaged property.

8. BEGIN AN INTERNAL INVESTIGATION

- **Determine the cause and extent:** Conduct an internal investigation to determine how the crime occurred, who was involved, and the full extent of the loss.
- **Interview witnesses and employees:** If applicable, interview witnesses, employees, or individuals who may have information regarding the incident.
- **Review security footage:** If available, review security camera footage for evidence or insights into the crime.

9. PRESERVE AND PROTECT EVIDENCE

- **Maintain chain of custody:** Ensure that any evidence (physical or digital) is properly preserved and documented to maintain the integrity of the investigation.
- **Avoid tampering:** Do not touch, alter, or dispose of evidence. Preserve the original condition of anything that may be relevant to the investigation or claim.

10. NOTIFY AFFECTED PARTIES

- **Inform employees (if necessary):** Notify your staff about the crime if it affects their work environment, benefits, or safety. Address concerns and provide guidance on next steps.
- **Notify customers or vendors (if necessary):** If the crime impacts your customers (e.g., stolen customer data, fraudulent transactions), notify them promptly and provide information on any protective measures (e.g., credit monitoring, incident resolution).

11. ASSESS POTENTIAL PUBLIC RELATIONS ISSUES

- **Communicate with the media (if necessary):** If the crime gains public attention, prepare a public statement. Work with PR professionals to manage any media inquiries or reputational damage.
- **Be transparent but cautious:** Share necessary details with stakeholders and the public, but avoid revealing sensitive information that could hinder the investigation or expose the company to further risk.

12. MONITOR AND PREVENT FURTHER LOSS

- **Monitor for signs of further crime:** Stay alert for any signs that the crime is ongoing or that there may be additional risks (e.g., continuing fraud, unauthorized access to systems).
- **Increase security measures:** Implement additional security measures, such as improving physical security (e.g., locks, alarms, surveillance cameras) or enhancing digital protections (e.g., firewalls, access control, encryption).

13. PLAN FOR RECOVERY

- **Repair or replace damaged property:** Begin the process of replacing stolen or damaged items, and repairing any physical damage to property.
- **Assess business continuity:** Develop a plan to minimize business disruption caused by the crime. This may include temporary changes to operations or emergency procedures.

14. REVIEW AND STRENGTHEN INTERNAL CONTROLS

- **Conduct a risk assessment:** After the incident, evaluate your internal controls, security policies, and procedures to identify vulnerabilities that were exploited during the crime.
- **Implement preventive measures:** Based on the findings, implement stronger security practices, improve employee training, and enhance fraud detection systems.