

10 Things Companies Can Do to Protect Employees Against Identity Theft



The threat of identity theft isn't limited to consumers. The sensitive personal information that companies routinely collect from their employees is also a juicy target for identity thieves, including Social Insurance Numbers, banking details, tax and benefit records, addresses, and copies of identification. There are 10 things employers should do to protect employee data from identity theft.

1. Limit the Personal Data You Collect

The more personal employee data you collect, the greater the danger of identity theft. So, limit yourself to only the essential data the company needs to perform employment functions. **Action Points:**

- Inventory the employee data collected by HR, payroll, benefits, IT, and third-party vendors.
- Document why each item is required.
- Consider ways to accomplish required purposes with less sensitive information.
- Stop collecting anything you can't justify, recognizing that "just in case" isn't justification.

2. Restrict Access to Sensitive Employee Information

Limit access to each item on your hopefully reduced employee data inventory.

Action Points:

Apply Least Privilege

Give employees and service providers access only to the records required for their duties. Review permissions regularly and remove access immediately when roles change or employment ends.

Separate & Encrypt Sensitive Records

Keep identity data out of shared drives and ordinary email. Encrypt it in transit and at rest, while maintaining secure, tested backups.

Monitor Access

Log downloads, exports, and unusual access to employee records. Investigate anomalies promptly.

3. Secure Accounts & Devices

Protect email, payroll, benefits, cloud storage, and administrator accounts.

Action Points:

- Use multi-factor authentication (MFA) and, where feasible, phishing-resistant methods to limit access to high-risk accounts.
- Enforce strong, unique passwords through a password manager.
- Keep operating systems and security tools current.
- Use device encryption, screen locks, endpoint protection, and remote-wipe capabilities on equipment that handles employee data.

4. Implement Extra Security for Payroll Workflows

Payroll deserves special scrutiny. Identity thieves may impersonate executives or tax agents to obtain employee tax forms.

Action Points:

- Require an out-of-band verification step before changing direct-deposit instructions, releasing bulk employee records, or sending tax documents; and
- Don't bypass normal approval processes when a request appears to come from an executive or CRA agent.

5. Implement Physical Controls

Incorporate physical controls into your identity theft prevention protocols.

Action Points:

- Store physical records in locked filing cabinets or secure rooms with restricted access.
- Position HR and payroll workstations so that personal information isn't visible to unauthorized individuals.
- Use key-cards, fob access, security codes, visitor logs, or other additional safeguards to secure areas containing highly sensitive information.

6. Limit Retention & Securely Destroy Employee Data

[Use and retain the personal information you collect from employees](#) for only as long as it remains necessary for business purposes and then securely destroy or erase it.

Action Points:

- Set a retention period for each item on your employee data inventory.
- When the retention period expires, lock and shred paper files and securely erase electronic records from active systems and backups.
- Verify that the data has been destroyed or deleted.

7. Provide Employees Identity Theft Prevention Awareness Training

Employees should receive training on identity theft and how to prevent it.

Action Points:

- Provide recurring training—annual awareness training isn't enough.
- Base training on realistic scenarios simulating real-life identity theft attacks, such as fake benefits enrolment notices, urgent payroll requests, etc.
- Train employees to verify unusual requests through a trusted channel, inspect links and attachments, refrain from approving unexpected MFA prompts, and report suspicious messages.
- Provide additional role-specific training to HR, payroll, finance personnel, executives, and IT administrators.

8. Extend Identity Theft Protections When Outsourcing Data to Third-Party Vendors

Companies [often share the personal employee data they collect with outsiders](#) like payroll vendors, benefits administrators, background-screening firms, and cloud providers.

Action Points:

- Review vendors' data security protocols before hiring them and on a regular basis thereafter.
- Include specific [data protections in vendors contracts](#), including permitted uses and requirements for safeguards, breach-notification, and data retention, deletion, and return.
- Require vendors to extend these requirements to any subcontractors to whom they entrust the data.
- Get the right to audit vendors' (and subcontractors') compliance with the above requirements.
- Require independent verification before the vendor changes an employee's banking, address, password-recovery, or benefits information.

9. Extend Identity Theft Protections to Remote & Hybrid Work Arrangements

Another potential blind spot is collection and use of sensitive employee data to carry out remote and hybrid work arrangements.

Action Points: Establish [data security ground rules for remote work](#):

- Require remote workers to use [approved data devices](#) and storage methods.
- Ban remote workers from printing sensitive records at home unless necessary, allowing family members to use work equipment, and discussing employee information in public spaces or within earshot of smart speakers.
- Provide a secure method for sending identity documents so remote workers don't have to use personal email.

10. Provide for Data Breach Notification

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) and provincial privacy laws [require companies to report and contain data breaches](#).

Action Points:

Promptly Notify Affected Employees

[Tell affected employees about the breach](#), the information involved, the company's response, and what employees should do next. Stick to the essential facts and avoid speculation or assignment of blame.

Help Affected Employees Secure Accounts

Instruct affected employees to change passwords, contact financial institutions, and review account and credit activity. Let them know they can report fraud to local police and the Canadian Anti-Fraud Centre, and should notify relevant government agencies, financial institutions, and credit bureaus as appropriate.

Offer Employees Practical Assistance

Depending on the circumstances and risks, consider offering affected employees credit-monitoring or identity-restoration support, paid time to replace identification, and a dedicated contact for questions.

Perform Post-Incident Review

Conduct a post-incident review, fix the control failure, update training, and confirm that copied data has been contained or deleted where possible.