

PERSPECTIVE

# Help Protect Your Employees' Identities If Their Information is Exposed in a Data Breach

---

**EQUIFAX**<sup>®</sup>

Workforce  
Solutions



Stories of large data breaches have become fixtures in the news. Cybercriminals are continuing to take advantage of increasing digital dependence to steal personal and financial information, **leading to a 22% increase in losses attributed to cybercrime last year: \$10.3B in 2022 to \$12.5B in 2023.**<sup>1</sup>

One of the ways these bad actors gain access to this data is through data breaches.



**\$10.3B**

lost from cybercrime in 2022

**\$12.5B**

lost from cybercrime in 2023

<sup>1</sup> FBI, Internet Crime Report 2023, December 2023

## REACHING RECORD HIGHS

[The Identity Theft Resource Center \(ITRC\)](#), a non-profit organization established to help minimize risk and mitigate the impact of identity compromise, found in its 2023 Annual Data Breach Report that, in the U.S., there were an average of more than twelve breach notices issued each business day. In fact, a total of 3,205 data compromises occurred in 2023, a 78% increase from 2022 and a new record, topping the previous all-time high of 1,860 set in 2021. In these breaches, more than 353 million individual credentials were compromised.<sup>2</sup>

12

average breach notices  
issued each business day

3,205

data compromises in 2023,  
the highest reported in a  
single year

353M

individual credentials were  
compromised

Through June 30 of 2024, there had already been 1,571 data compromises reported impacting an estimated 1.07 billion victims, a 14% increase in compromises compared to this same period in 2023.<sup>3</sup> With these lofty numbers, it is important to consider how you can help your employees if their personal information does become exposed.

<sup>2</sup>ITRC, 2023 Annual Data Breach Report, January 2024. <sup>3</sup> ITRC, H1 2024 Data Breach Report, July 2024.

## POTENTIAL RISKS OF A BREACH

Once a data breach has occurred, your employees' credit profiles and identities can be at risk. With their personal information compromised, they may be at greater risk of having their accounts hijacked, credit profile impacted, identities stolen, and more. **Criminals typically don't wait around once they have stolen credentials.**

It could only be a short time before an employee's personal information could possibly be used for:



Accessing existing credit cards, bank accounts, or loans to buy goods or services.



Opening a new bank account in their name to store and/or transact criminal proceeds.



Trading on the dark web.



Applying for government benefits.



Applying for false identity documents.



Changing passwords to accounts so access is denied.



Applying for new credit cards or loans in their name.



Applying for utility accounts such as phone or electricity.

## An Identity Theft Protection Benefit Can Help

An identity theft protection benefit can help you stem the tide for your employees against the growing threats of identity fraud and help lighten the burden of monitoring and safeguarding their accounts, credit, and digital identity on their own.

Identity theft protection cannot stop your employees' identities from being stolen in a breach, but it can help them better defend against fraud and monitor their accounts for suspicious behavior.

# IDENTITY THEFT PROTECTION FEATURES



## **Fraud alert and credit report lock tools**

to help give your employees the ability to lock access to their credit reports and to encourage lenders to take extra steps to verify their identity before extending credit.



**Credit monitoring and alerts** so that they are made aware of key changes to their report.



## **Financial account monitoring and alerts tools**

that can help alert your employees of potentially fraudulent activity across multiple accounts such as credit cards, banking, and investments.



**Monitoring of networks outside of the traditional banking system** that will alert them if new or blocked subprime lending activity using your identity is detected, so they can take action to verify it or deny it.



## **Digital security and privacy tools like VPN, anti-virus protection, and password managers**

to help better protect their own and their family's devices, personal information, online accounts, and digital identities.



**Live customer service agents available 24/7/365.**

## NEXT STEPS FOR VICTIMS OF IDENTITY FRAUD

If an employee or someone covered in their family does become a victim of identity fraud, an identity theft protection service should have:



### **Highly-skilled restoration specialists**


to help them restore their identities as quickly as possible.



**Identity theft insurance** for certain out-of-pocket expenses they may face as a result of having their identity stolen.

For more information regarding steps your employees can take if their information is in a data breach, check out:

[My information was exposed through a Data Breach — what can I do?](#)



If you do not currently offer identity protection service as a benefit and are interested in learning more about where to start, what options are available, and how it can help you better protect your employees and their families from identity theft and fraud, visit:

**[workforce.equifax.com](https://workforce.equifax.com)**

The information provided is intended as general guidance and is not intended to convey any tax or legal advice. For tax or legal information pertaining to your company and its specific facts and needs, please consult your own tax advisor or legal counsel. Links to sources may be to third party sites. We have no control over and assume no responsibility for the content, privacy policies or practices of any third party sites or services.

Copyright © 2024, Equifax Inc., Atlanta, Georgia. All rights reserved. Equifax is a registered trademark of Equifax Inc. The Work Number is a registered trademark of Equifax Workforce Solutions LLC, a wholly owned subsidiary of Equifax Inc EWS-1469026212



**EQUIFAX®**

**Workforce  
Solutions**