



**EBOOK**

# 5 Things to Look for in an Identity Theft Protection Benefit

**EQUIFAX**<sup>®</sup>

| Workforce Solutions



Fraudsters are taking advantage of increasing digital dependence to steal personal and financial information—

***victimizing 40 million U.S. consumers in 2022 for \$43 billion in identity fraud losses.<sup>1</sup>***

No one is immune to identity theft and if it becomes fraud, the effect can be wide-reaching regardless of income, education, or generation. Criminals are using cyber-attacks, digital account takeovers, and social engineering to perpetrate theft and fraud against employers and employees, causing them to have to defend multiple fronts to help secure their critical information and better protect against financial loss and stress.



A **best-in-class 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. It can also aid your HR team in helping recruit and retain talent by validating your reputation as a more generous and supportive employer.

Most identity theft protection benefit offerings in the market today will claim to help your employees with prevention, detection and resolution, but there are important nuances to consider. For example, is the solution focused on stopping your employees' identity from being stolen, or do they also help prevent stolen identities from being used for fraud? Or how will the benefit help keep the employees' loved ones safe from fraudsters?

Here are five essential qualities you should look for in an identity protection benefit to help give your employees and their families more of the protection they need and the greater peace of mind they deserve.



# #1

## PROTECTION FROM DAY 1

Your employees may not immediately activate their identity protection service, but this shouldn't keep their identity and personal information potentially exposed. After an employee signs up for identity protection as a benefit, it should immediately begin monitoring the personal and credit information of the subscriber and alert them if suspicious activity is found. You should look for at least 1-bureau credit monitoring, dark web monitoring, and **subprime loan monitoring**.

For a top-quality service, monitoring for the family members in the employee's enrollment file should also begin at signup.

And speaking of family protection...



**Criminals don't wait  
around for someone  
to activate their  
protection plan**



## **What is... Subprime Loan Monitoring?**

Monitors networks outside of the traditional banking system for transactions like payday, non-prime, high-cost installment, rent-to-own, and other loans. If new or blocked subprime activity using your identity is detected, it will alert you so you can take action to verify it or deny it.



# #2

## PROTECTION FOR THE WHOLE FAMILY



Identity theft can affect anyone—from infants to seniors. ***\$688 million was lost to child ID fraud in the past year and takes 78% longer to resolve than adult ID fraud.***<sup>2</sup> While adults may be targeted by identity thieves for the money in their accounts, a child represents an entirely different type of opportunity—a clean slate for opening new lines of credit that may go unnoticed for years. A truly effective identity protection service should have robust features to help identify and mitigate these risks.

But children are not the only family members that should be considered.

**Family members, including children, are just as vulnerable as adult employees**



***In 2022, fraud victims over the age of 60 reported fraud losses of \$3.1 billion to the FBI's Internet Compliance Center (IC3). This represents a 72 percent increase over losses reported in the previous year.<sup>3</sup>***



Seniors should not be left behind in an employee's identity protection benefit, and you should prioritize those services that offer them the ability to add their older family members to their plans.

An effective identity protection service should have features to help employees protect their entire family from the issues that can plague victims of fraud. This should be more than just dark web monitoring, it should also include features that help employees protect their family's credit futures like, credit monitoring and credit lock features for adult and child family members, family alert sharing, and the ability to add older family members who may not live with them to their plans.





# #3

## CYBERSAFETY ACROSS DEVICES

Now more than ever it is important to arm employees with digital security and privacy tools like VPN, anti-virus protection, and password managers to help protect their own and their family's devices, personal information, online accounts, and digital identities.

Offering access to digital identity and device security features can help employees:

- safeguard their devices against e-threats
- set parental controls on their children's devices
- keep their and their family's online activity and personal information more private
- generate, manage, and store distinct and complicated passwords

These tools should be available on numerous devices to help employees responsibly protect both their corporate and personal devices from vulnerabilities that can lead to data compromises, theft, and fraud.

***Americans experienced \$10.3B in losses due to cybercrime in 2022  
(Up 49% from 2021)<sup>3</sup>***

# #4

## FINANCIAL FRAUD PROTECTION

*Traditional identity fraud losses totaled \$20.3 billion in 2022<sup>1</sup>*

While the digital threat landscape increases with our greater digital dependence, traditional financial fraud continues to lead to mountainous losses. Because of this, elements like **credit report locks** and **fraud alerts** remain essential to true identity theft and fraud protection. These tools can 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.

Additionally, an all-in-one financial account monitoring and alerts tool can help your employees receive alerts on potentially fraudulent activity across multiple accounts such as credit cards, banking, and investments. Receiving timely alerts helps your employee to immediately start to investigate and act to mitigate these activities.

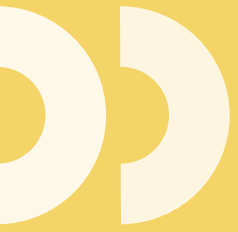


## **What is... a credit lock?**

Credit report locks are desktop or mobile app-enabled and allow your employees to lock and unlock their credit reports using identity verification techniques such as usernames, passwords, and Touch ID or Face ID technology.

A credit lock will not hurt their credit. It will help prevent access to their credit reports to open new credit accounts. Since potential creditors can't check their credit reports, a lock helps better protect against identity thieves opening new accounts in their name. If your employees legitimately want to apply for credit, they will need to unlock their credit report.

Their credit reports must be locked separately at each nationwide credit bureau (Equifax, Experian and TransUnion). If you choose an identity theft protection service that has a multi-bureau lock feature, your employees have the ability to lock their credit reports for more than one of the bureaus within the service.



## What is...a fraud alert?

A fraud alert is a notice that is placed on your employee's credit report that alerts credit card companies and others who may extend them credit that they may have been a victim of fraud, including identity theft. Acting like a "red flag" to potential lenders and creditors, it encourages them to take extra steps and contact your employees to verify their identity before extending credit in their name.

**Learn More about  
Identity Theft Protection**



# #5

## SUPPORT WHEN THEY NEED IT


It is important for employees to have support from a provider that is available when they need it and with service that will meet or surpass their expectations. At a minimum, they should expect to be able to speak to a live customer service agent 24/7/365.

If they or someone in their family does become a victim of identity fraud, their service should have certified resolution specialists ready to help them manage their case until their identity is restored, even for pre-existing conditions.

These services should include:

- Placing phone calls, sending electronic notifications, and helping prepare appropriate documentation on behalf of your employee, including dispute letters and defensible complaints to appropriate agencies and financial institutions.
- Helping issue fraud alerts, security freezes, and victim's statements, when necessary, with the three consumer credit reporting agencies.
- Helping contact, follow up on, and escalate issues with affected agencies, creditors, financial institutions, etc., to assist in reinforcing your employee's rights.

**Identity theft  
and fraud is not  
something to go  
through and  
resolve alone.**



As focus on employee benefits intensifies around financial wellness, identity theft protection is becoming less of just a nice to have. By helping contribute to your employees' financial health through impactful benefits, you can help position your company as an organization that takes better care of its employees inside and out of the office. This can help strengthen your efforts in recruiting and retaining top talent. While you shop for the right solution to better safeguard the identities of your employees and their families, consider the 5 above ingredients as essential.



## Uniquely Designed to Watch Over Your Workforce

Contact us today to learn how to help your employees and their families fight against identity theft.

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



The information provided is intended as general guidance and is not intended to convey any tax, benefits, or legal advice. For 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 © 2023, Equifax Inc., Atlanta, Georgia. All rights reserved. Equifax and ID Watchdog are registered trademarks of Equifax Inc. WF-13367477