



IdentityForce.™

EXECUTIVE SUMMARY

# 2017 STATE OF PROGRESSIVE EMPLOYEE BENEFITS

SURVEY RESULTS FROM THE HR FRONTLINE

## SURVEY OVERVIEW

The first IdentityForce Progressive Benefits Survey was conducted during the second quarter of 2017. It polled 105 HR professionals across the U.S. about their current and future plans to invest in progressive benefits programs for their employees. Half of the respondents worked at companies with more than 5,000 employees, and 64% of respondents were identified as managerial professionals and above.

## SURVEY RESULTS

### Who is leading the effort to secure employees' personally identifiable information (PII) inside your organization?

HR	66.20 %
IT	63.38 %
Finance	8.45 %
Unsure	9.86 %
Other	12.68 %

### Nearly 68% of HR Professionals Consider Identify Theft Protection an Increasingly Important Employee Benefit

When competing for and retaining professional talent and building a distinct company culture, 67.5% of Human Resources (HR) executives are either actively looking or currently evaluating identity theft protection as a progressive employee perk. It also appears that Information Technology (IT) teams are increasingly looking at identity protection as an important line of defense against potential security data breaches.

The fact that HR and IT teams are collaborating on identity theft is one of the key highlights of a recent research study released by IdentityForce, a leading provider of proactive identity, privacy, and credit protection for individuals, businesses, and government agencies. Other key takeaways from the survey include the following:

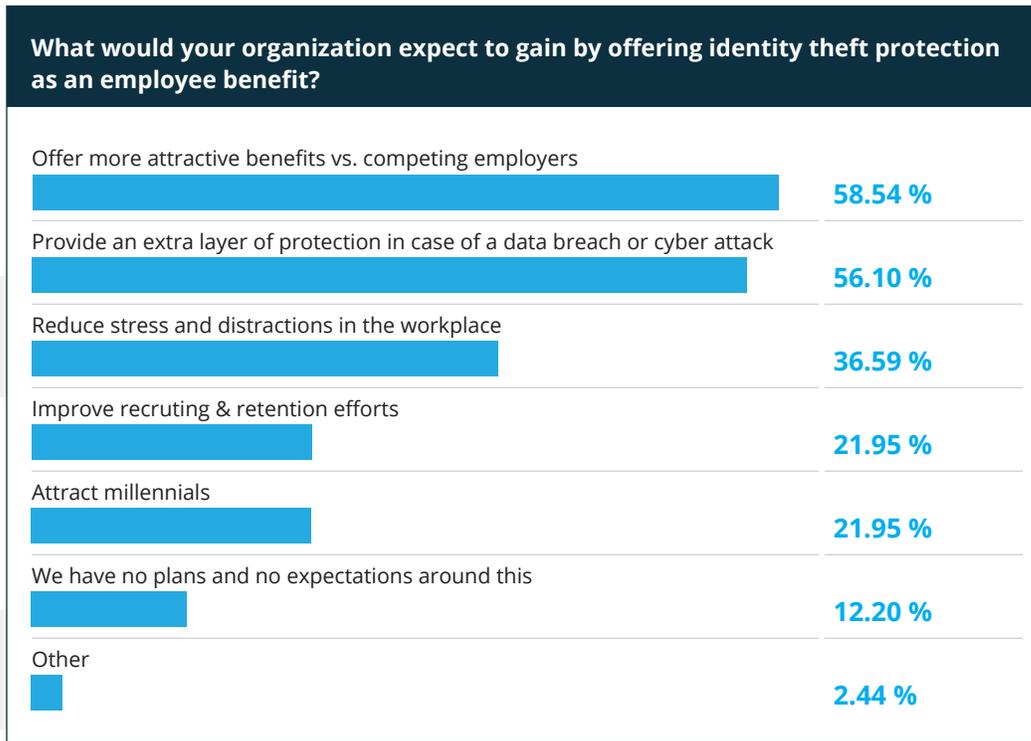
- Only half of companies surveyed currently offer identity theft protection to their employees, suggesting that most firms may be unsure when to implement an identity theft protection strategy.
- Information Technology (IT) and HR functions nearly equally share in driving the effort to secure employees' personally identifiable information inside their organizations, at 66.2% and 63.4%, respectively. (See **Figure 1**)
- Most respondents (58.5%) cite the need to offer identity theft protection as an attractive employee benefit to compete with other employers for talent acquisition and retention. This statistic is nearly matched by a majority of respondents (56.1%) who identify the need to provide an extra layer of protection in the case of an enterprise-level data breach or cyber attack. (See **Figure 2**)

**FIGURE 1**

### Understanding the business ecosystem involved in identity protection

**FIGURE 2**

**Why companies would consider offering an identity theft protection benefit for employees**



## BUILDING AN EMPLOYEE “EXPERIENCE” WITH PROGRESSIVE BENEFITS

The need to attract, retain, and motivate talented employees is a constant in any organization. One of the major new initiatives in HR management is focused on designing a compelling “employee experience,” rather than checking the boxes of traditional gym memberships and 401(k)s. Today’s worker’s, particularly in the younger ranks, want to feel that companies care about their well-being — physically, emotionally, and financially. No wonder that 83% of HR executives say employee experience is either very important or important to their organization’s success.<sup>1</sup>

*Today’s worker’s, particularly in the younger ranks, want to feel that companies care about their well-being — physically, emotionally, and financially.*

The recent growth in progressive benefits programs, such as offering unlimited vacation time, pet insurance, identity theft protection, student loan repayment, onsite dry cleaning, and paid volunteering is an outgrowth of this desire among companies to meet employees on their terms, according to a recent research study from Willis Towers Watson. The global benefits advisory firm reported that 92% of their survey respondents view voluntary benefits and services as being “at the forefront” of their strategic thinking and important to their employee value proposition, up from 59% in 2013.<sup>2</sup>

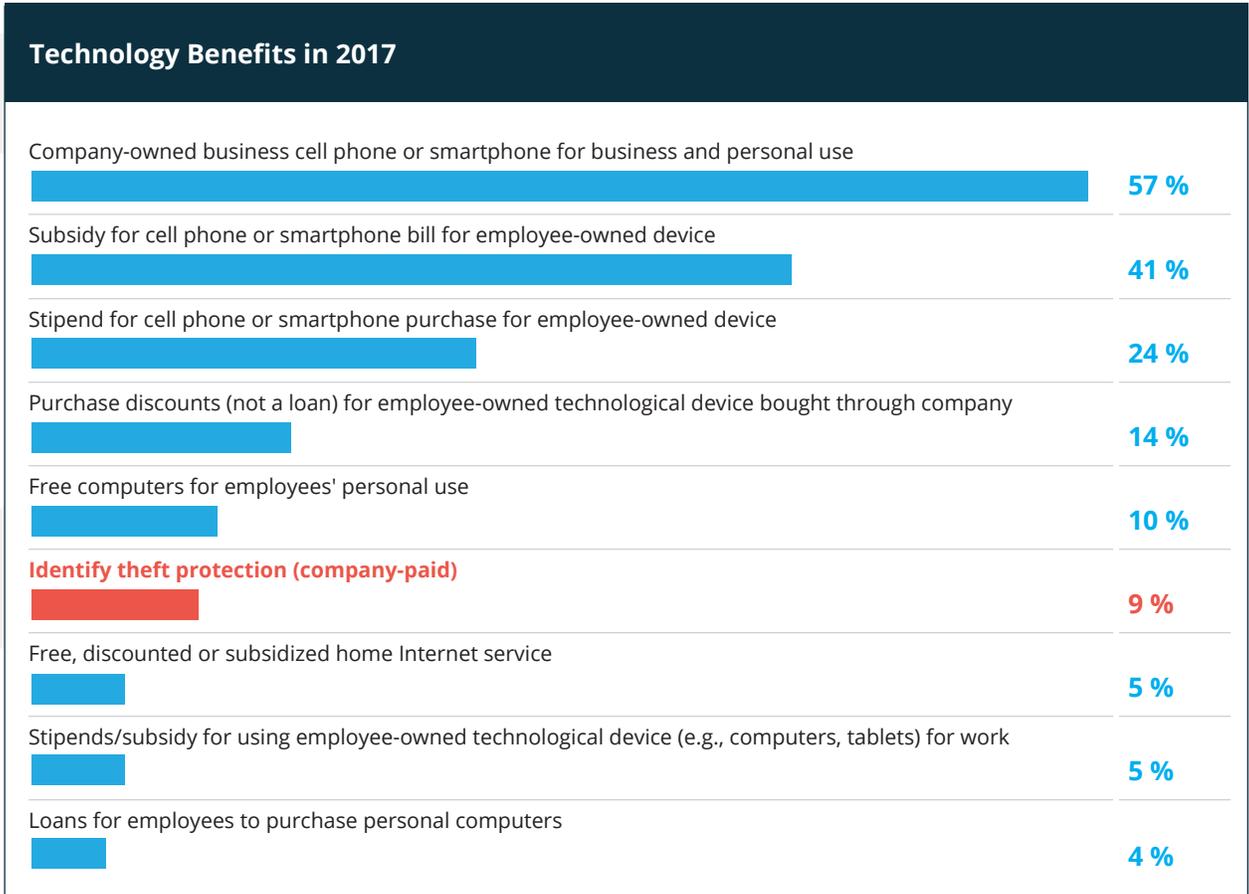
Technology-related benefits remain a popular trend at most companies, according to the Society of Human Resource Management (SHRM). Notably, SHRM lists company-paid identity protection for the first time in its 2017 Benefits Survey, reported by 9% of SHRM’s Benefits Survey respondents. (See **Figure 3**)

1. “4 Top Leadership Trends for HR Managers in 2017,” Causecost.com blog post, January 18, 2017.

2. Willis Towers Watson, Infographic: *Key insights from the 2016 Voluntary Benefits and Services (VBS) Survey.*

FIGURE 3

Over a 5-year period, Identity Theft Protection appeared for the first time in 2017 as a new benefit being offered by companies (survey conducted by SHRM to more than 3,000 HR professionals)



Source: SHRM, 2017 Employee Benefits: Remaining Competitive in a Challenging Talent Marketplace

Given the proliferation of company paid or subsidized technology benefits for use at and outside of work, identity theft protection would appear to be an important and growing employee perk.

## DEDUCT THE COST

### Did You Know?

The U.S. IRS treats ID theft protection as a non-taxable, non-reportable benefit that companies can offer.

## ADDITIONAL RESOURCES

HR People + Strategy | [5 Tips for Securing BYOD \(and Company\) Data](#)

Voluntary Benefits Magazine | [3 Reasons Why Mobile-friendly Benefits Matter](#)

Employee Benefit News | [How Employers can Protect Workers from Identity Theft](#)

## EVOLVING WORK-LIFE PREFERENCES

The move to enhance employee benefit plans with financial wellness and identity theft protection programs is driven in part by the financial concerns and shifting work-life preferences of workers, as well as the strategic imperative of companies of all sizes to protect themselves from value-destroying losses.

- **Financial worries stress employees and lead to productivity losses.** Money is the number one source of stress for most workers, according to a study from Guardian Life Insurance,<sup>3</sup> which can lead to an array of health ailments. And identity theft is a major catalyst for long-term stress, as 66% of all data breach victims reported experiencing direct financial losses, and 48% believe that their identity was at risk for years beyond a single data-breach incident.<sup>4</sup> No forward-looking organization wants their employees to experience the stress and strain from personal financial losses, as the toll on workers and business productivity could be detrimental.
- **Data breaches from individual employee BYOD devices.** Employees of the future want to have truly flexible work schedules, working anytime, from anywhere. Thus, many organizations are relaxing restrictions of which phones and computers their employees can use when logging into company networks — even sanctioning BYODs (bring your own devices) when working both inside and outside the office. This potentially raises the specter of endpoint security risks for IT departments that can be mitigated by enterprise threat detection and containment at the employee layer. IT managers likely will want to explore end-to-end solutions that do this without adding to their IT budget, staffing needs, or workflow.

To attract new talent and create a modern, competitive organization, employee benefits must be assessed along a continuum of how they can enhance the employee experience. Companies must protect their most valuable assets — their employees — from security intrusions that, if successful, could threaten their financial well-being, and possibly lead to value-destroying losses at the enterprise. To this end, the IdentityForce survey was notable in showing that:

- 55% of respondents already are, or might consider adopting, identity theft protection
- 22% of those considering it plan to do so in the next 12 months

On the menu of today's available progressive benefits, perhaps none is more important to a company than monitoring, detecting, and responding to the theft of personally identifiable information. It's becoming even more of a corporate directive with the ever-growing number of employee digital devices used inside and outside the worksite and ubiquitous data breaches.

3. Guardian Life Insurance, [Fourth Annual Workplace Benefits Study, 2016](#).

4. Small Business Trends blog post, ["Keep it Down! Employees Rank Workplace Distractions as Biggest Beef," June 14, 2016](#).

To learn more about how IdentityForce's proven identity, privacy, and credit security solutions can add value to your corporate employee benefits program, please sign up for a [Free Business Trial](#) or email us at [info@identityforce.com](mailto:info@identityforce.com).

### About IdentityForce

For nearly 40 years, IdentityForce, Inc. has provided best-in-class, highly scalable, award-winning identity theft, privacy, and credit protection solutions to consumers, businesses, and government agencies. A pioneer of identity protection, IdentityForce's innovation and customer-centric approach has made the company a trusted partner for both organizations and individuals. IdentityForce also provides custom-tailored programs to organizations enabling them to build closer relationships and additional revenue streams. In 2015, the U.S. government awarded IdentityForce elite Tier-One status as an approved provider of identity protection services for data breaches affecting over 21.5 million people. Visit [www.identityforce.com](http://www.identityforce.com) to learn more.



Find IdentityForce on:



©2017 IdentityForce, Inc. All other trademarks or trade names are properties of their respective owners. All rights reserved.