Exclusive Insight:
THE FUTURE OF EMPLOYEE BENEFITS

Presented by SONTIQ™

IdentityForce® CYBERSCOUT® EZShield®

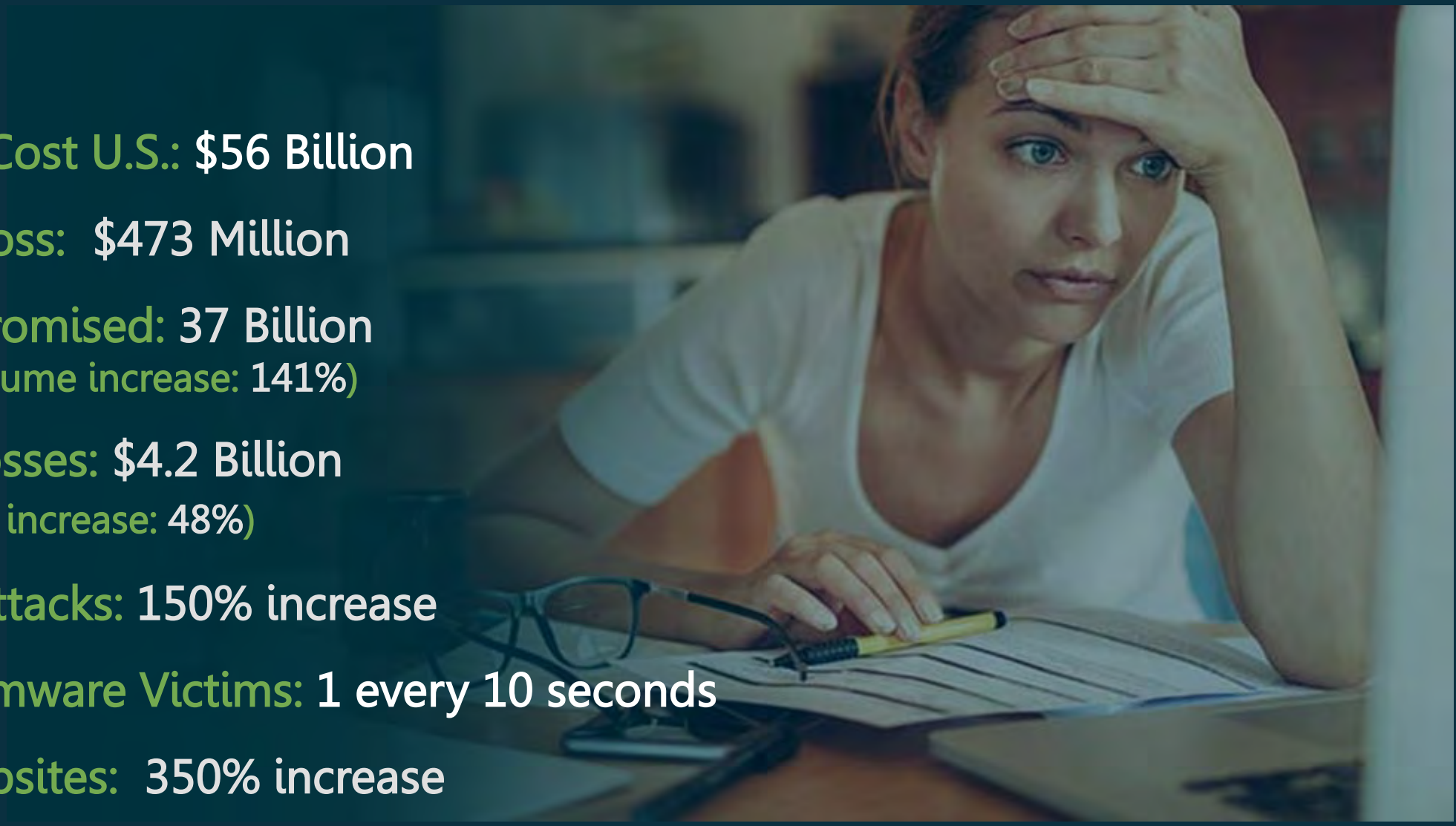
SONTIQ™
Intelligent identity security.

WELCOME

Today's Webinar Speaker

Donna M. Parent
Chief Marketing Officer

A VOLATILE YEAR FOR EVERYONE



- Identity Fraud Cost U.S.: $56 Billion
- COVID Fraud Loss: $473 Million
- Records Compromised: 37 Billion
  (Year over year volume increase: 141%)
- Online Scam Losses: $4.2 Billion
  (Complaints to FBI increase: 48%)
- Ransomware Attacks: 150% increase
- New US Ransomware Victims: 1 every 10 seconds
- Fraudulent Websites: 350% increase

RISE OF THE REMOTE WORKFORCE

88%

of organizations had employees work from home during the pandemic

SOURCE | Gartner

44%

U.S. employees want to continue working remotely

SOURCE | Gallup

THE PRICE OF CONVENIENCE

61%

Security Professionals say personal devices pose the biggest wireless threat to companies

33%

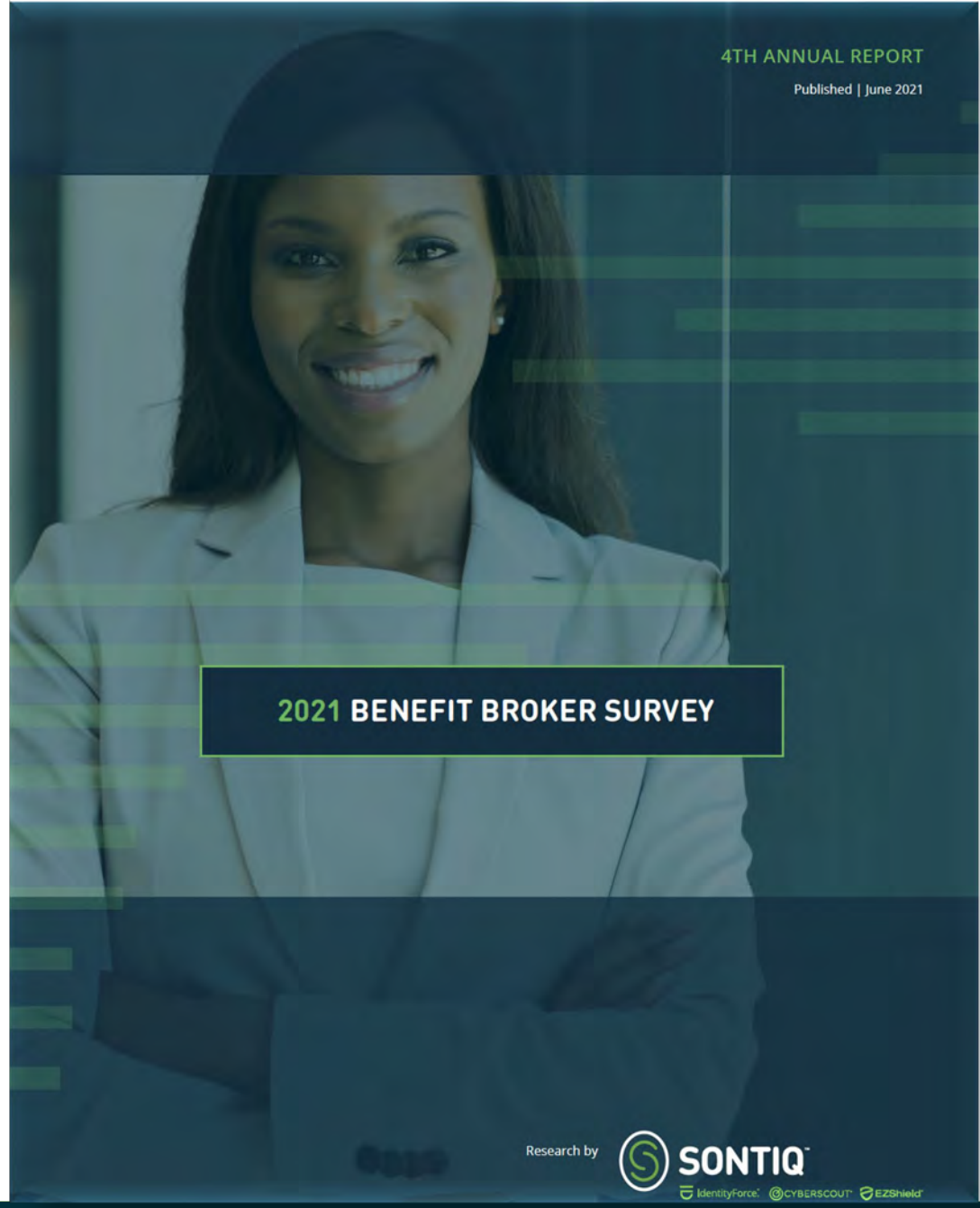
Security Professionals confident they can prevent a wireless/ Wi-Fi attack

SOURCE | 2020 Internet of Evil Things

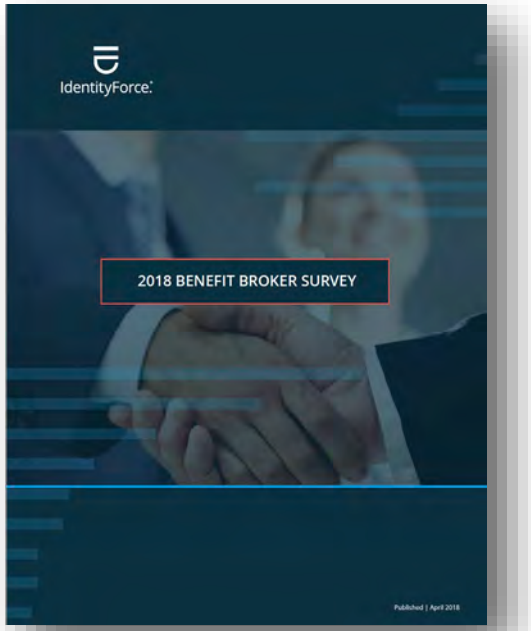
4TH ANNUAL | BENEFIT BROKER SURVEY REPORT

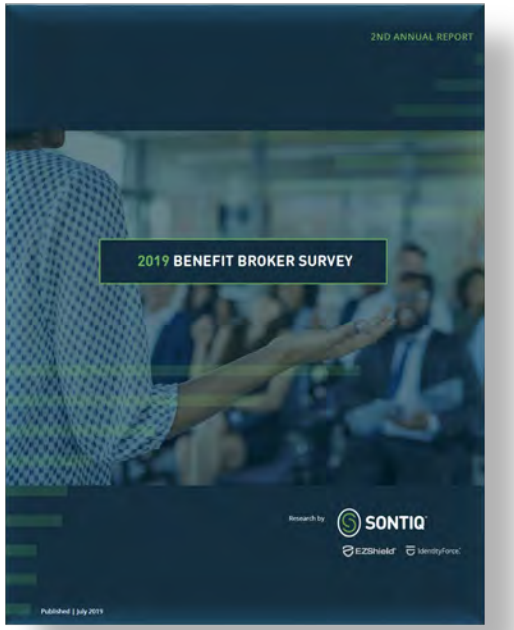
EXCLUSIVE

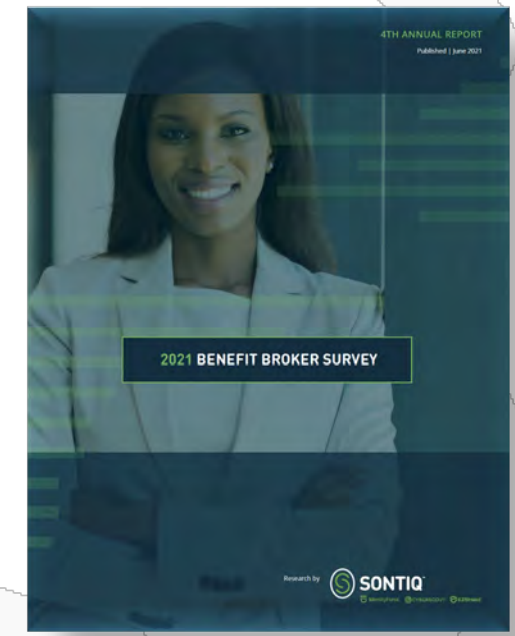
Feedback from **250+** Benefit Brokers & Advisors



A TRADITION OF PRIMARY RESEARCH







> *"The rapid move to virtual has attracted increasingly sophisticated criminal activity in identity theft, ransomware, and cyber fraud."*

ACCESS ON THE GO

KEY FINDING

Mobile App Access to Benefits (91%) has become a table-stakes benefit, with clients reporting that having a mobile app is "very important" or "extremely important," increasing by 8% year over year.

218B

New apps downloaded in 2020 alone

275%

Increase in time spent on business apps (Q4 2019 - Q4 2020)

SOURCE | App Annie State of Mobile

TELEMEDICINE: THE DOCTOR IS IN

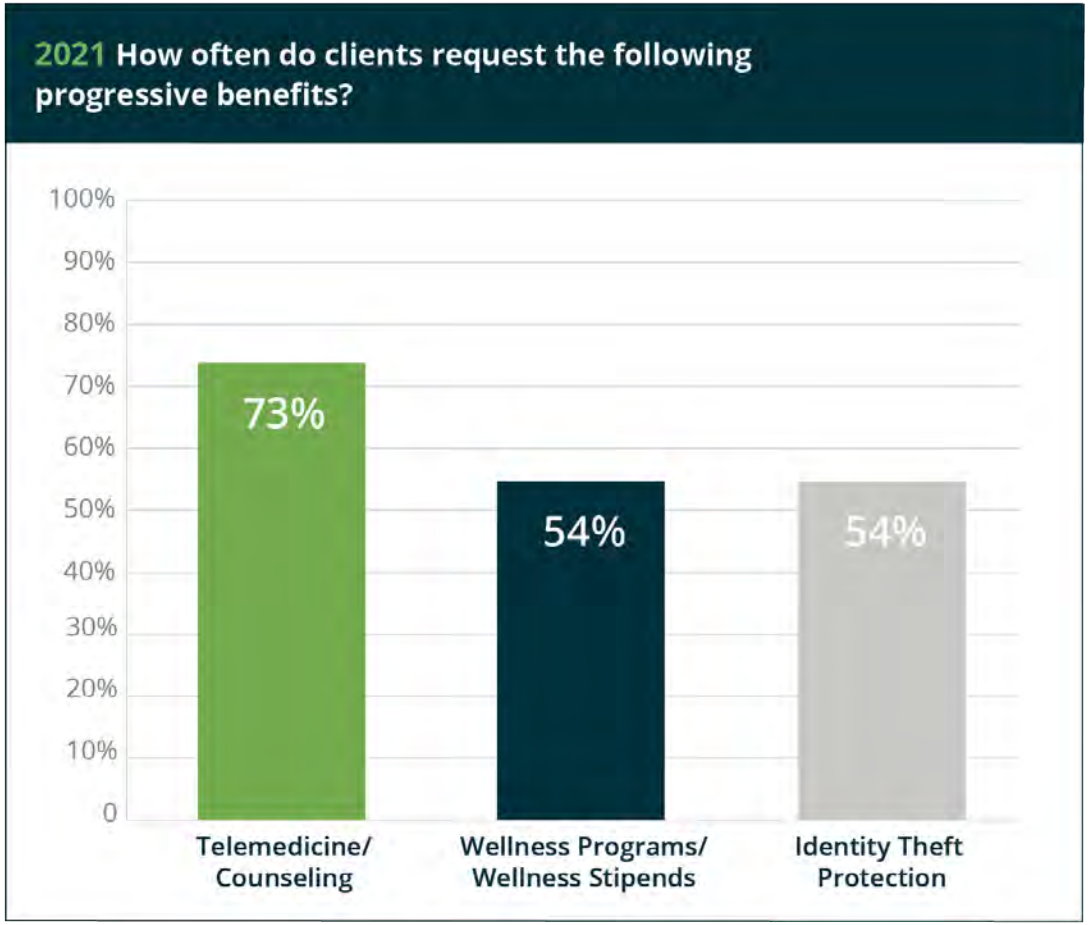


Figure 2 | The progressive benefits most requested by organizations

EMPLOYEE WELLNESS REMAINS ON TOP

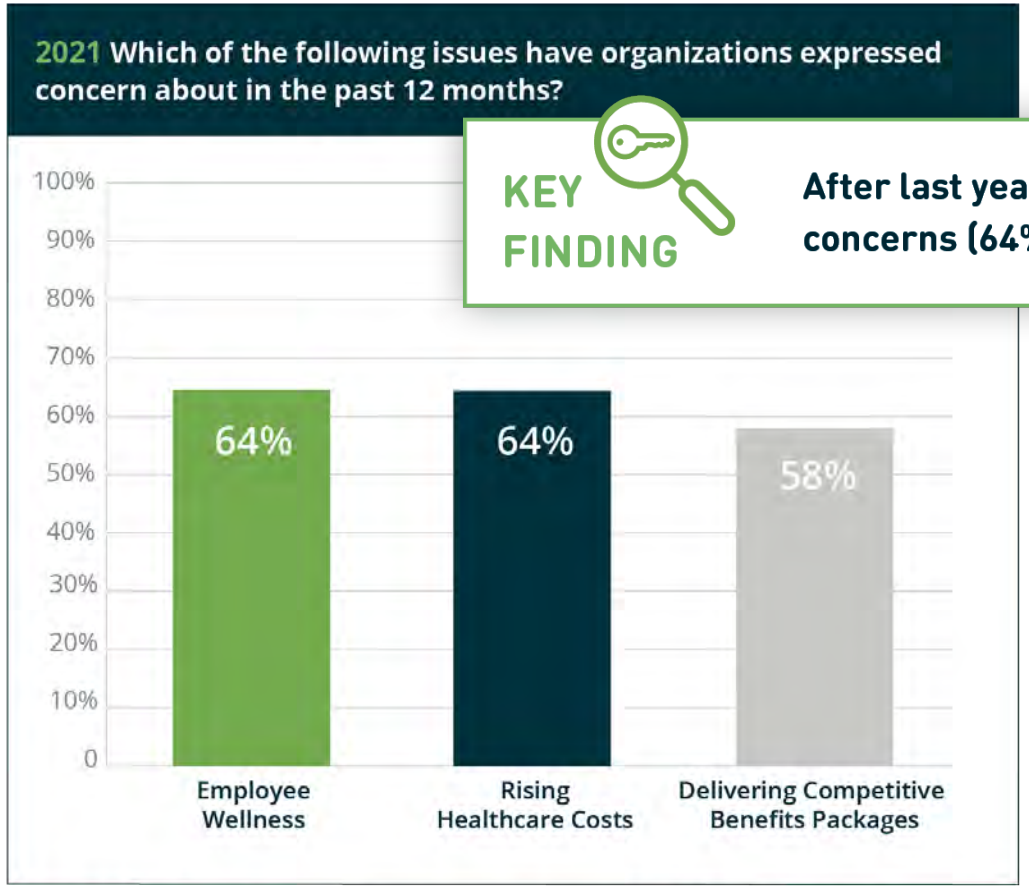


Figure 1 | The most pressing concerns expressed by HR and Benefits pros

KEY FINDING

After last year's rise to the top, Employee Wellness continued to lead employer concerns (64%), with Talent Shortages no longer a primary issue.

IDENTITY THEFT & CYBER THREATS

KEY FINDING

Digital security is a growing concern. For the third year in a row, more than half (54%) of clients are requesting Identity Theft Protection from their brokers. Cyber Threat Protection is being requested by 51% of broker clients.

SPECIALIZED CYBER PROTECTION

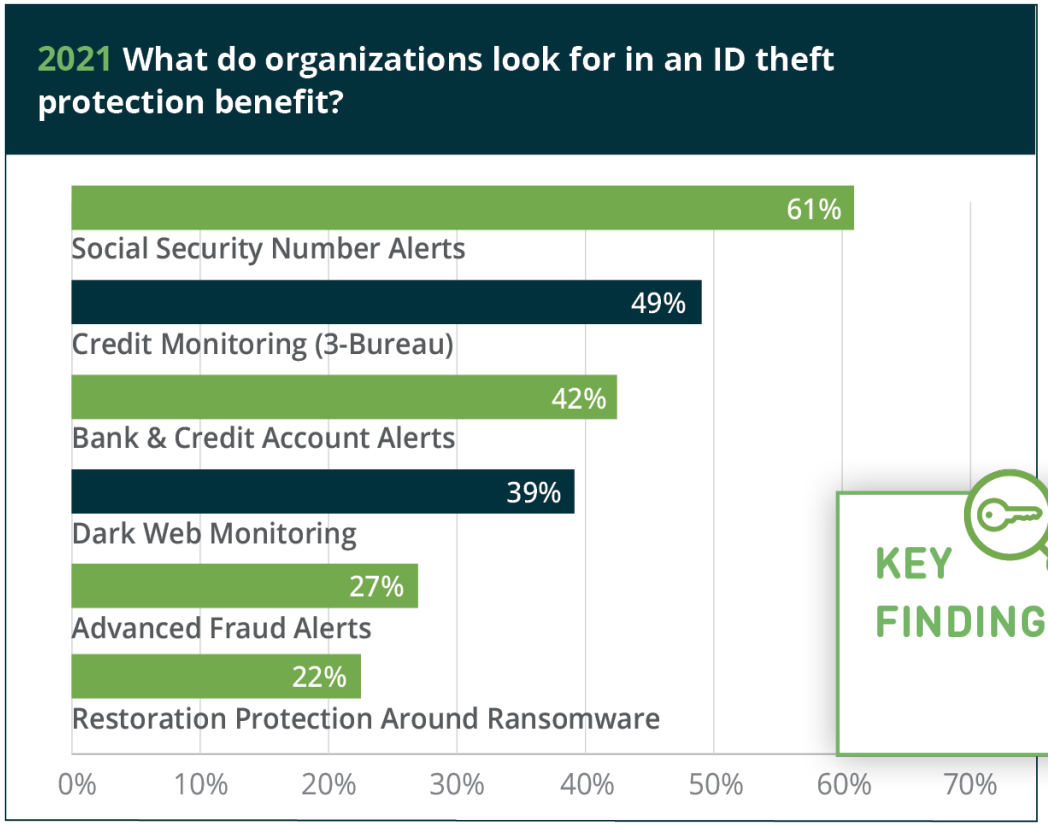


Figure 6 | Most requested identity theft protection features

90%

of consumers believe they can become a victim of ID theft or cybercrime at any moment

SOURCE | HelpNetSecurity

KEY FINDING

Organizations are broadening their expectations from identity theft protection, with Social Security number monitoring (61%) leapfrogging credit alerts (49%) as the top ID theft benefit request, and restoration protection around ransomware entering the list for the first time.

EMPLOYEE RISK = EMPLOYER RISK

45%

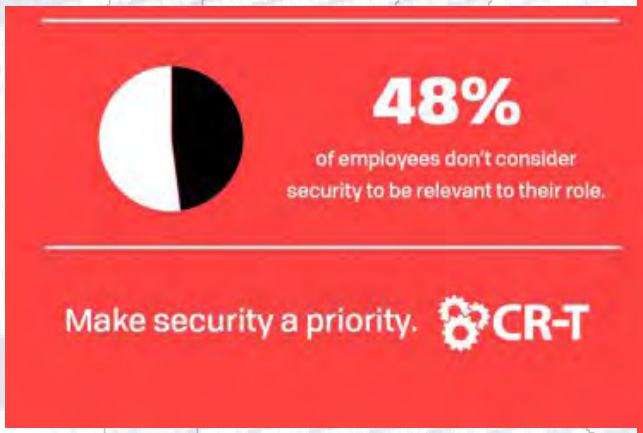
of cybersecurity leaders have connected to *public* Wi-Fi without using a VPN

Source | Constella Intelligence

1/3

change password after a data breach

Source | Carnegie Mellon University's Security and Privacy Institute (CyLab)



DATA BREACHES AFFECT EVERYONE

- 1 in 3 breach victims suffers identity theft
- Breaches including sensitive PII: 80%
- Top 2021 data exposed:
  - Name: 96% (97% in 2020)
  - Date of Birth: 60% (49% in 2020)
  - Medical History: 48% (22% in 2020)
  - Home Address: 39% (54% in 2020)
  - Full SSN: 33% (41% in 2020)

EXPERT ASSISTANCE FOR BROKERS

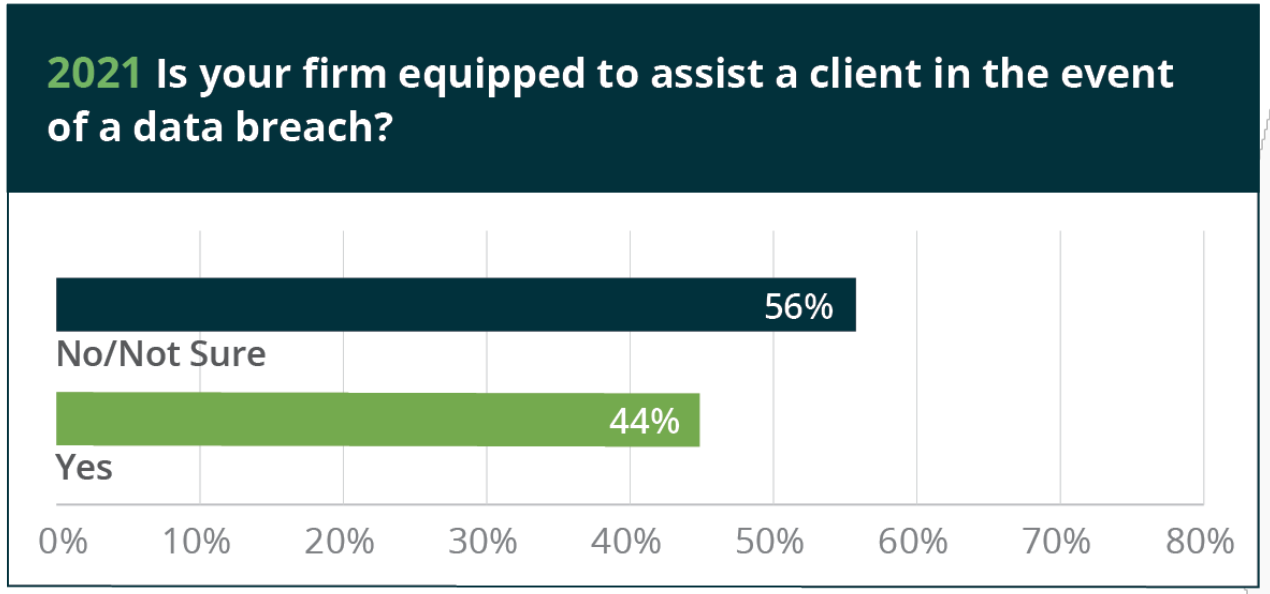


Figure 7 | Helping clients if employee or customer information is compromised

51%

of organizations don't believe they're ready or would respond well to a cyber attack or breach event

SOURCE | FireEye

KEY FINDING

In the face of increasing cyberattacks and the outgrowth of many new types of online scams, less than half (44%) of benefit brokers say they are ready to help their clients handle a data breach.

SONTIQ™

Intelligent identity security.

ACTIONABLE TIPS

Protect ALL the identities you're responsible for

8 WAYS TO SHUT DOWN HACKERS

SONTIQ
IdentityForce. CYBERSCOUT EZShield

1. **Update Software** | Use anti-virus, anti-keylogging, anti-phishing, and other security software — including mobile security — and keep it updated.
2. **Change Passwords** | Keep them complex, unique, & change them regularly, and don't forget home devices like TVs, smart thermostats, or video doorbells.
3. **Don't Save Details** | Turn off autocomplete, don't save payment details, and clear browsing history to keep information away from hackers if they do manage to breach your device.
4. **Be Cautious of Links** | Phishing emails lead to most data compromises — if you're not expecting it, just delete it. Don't respond or "play" with the scammer, giving them confirmation your email is valid.
5. **Safe Wi-Fi usage** | Don't connect to public or unsecure wi-fi, and use a Virtual Private Network (VPN) especially on mobile devices.
6. **Two-factor authentication (2FA)** | Always use 2FA when it's available — and if it's not, think twice about using that platform.
7. **Limit Personal Sharing** | Play it casual on social, while gaming, even on professional networking sites to keep your details safe from scammers who may use social engineering tricks to break into your accounts or scam your friends.
8. **Monitor Your Information** | Monitor your credit, Social Security number, and personal information on the Dark Web, so you get early indicators of potential issues.

5 WAYS TO SECURE MOBILE DEVICES

SONTIQ
IdentityForce. CYBERSCOUT EZShield

1. **Keep network settings secure and password protected**
   Remote workers increase security risks for businesses; scammers are targeting employees through Business Email Compromise and spear phishing
2. **Don't duplicate your passwords**
   Use strong and unique passwords for every account so credential stuffing attacks are stopped in their tracks, and don't share passwords between personal and business accounts
3. **Protect ALL your devices**
   - **Personal and work:** smartphones, laptops, tablets, wireless printers,
   - **Plus:** cars, appliances, fitness trackers and other wearables, lighting, healthcare, home security, any smart device connected to your network
4. **Keep tabs on your apps privacy & security settings**
   Especially apps running connected devices
5. **Teach children to keep devices safe & secured**

4 STEPS TO TAKE IMMEDIATELY IF YOUR ID IS STOLEN

1. Start a Paper Trail

- Document all activity related to clearing your name
- Log phone calls by date, time, resolution status
- Create calendar with critical dates that must be met to report fraud

2. File Reports

- Report the fraud directly to all companies involved
- Report identity theft to your local police
- Create identity theft report with FTC

3. Monitor Transactions

- Close or freeze any impacted accounts to stop new activity
- Turn on transaction monitoring for any open accounts

4. Control Your Credit

- Place fraud alerts and credit freezes with major credit bureaus
- Watch credit reports for suspicious activity and new account openings

It can take
100-200 Hours
and **6+ Months**
of work to restore
your identity after
a single incident

YOU DON'T HAVE TO DO IT ALONE

Consider Identity Theft Protection
with Restoration Services
for your employees
and their families

SONTIQ™
IdentityForce® CYBERSCOUT® EZShield®

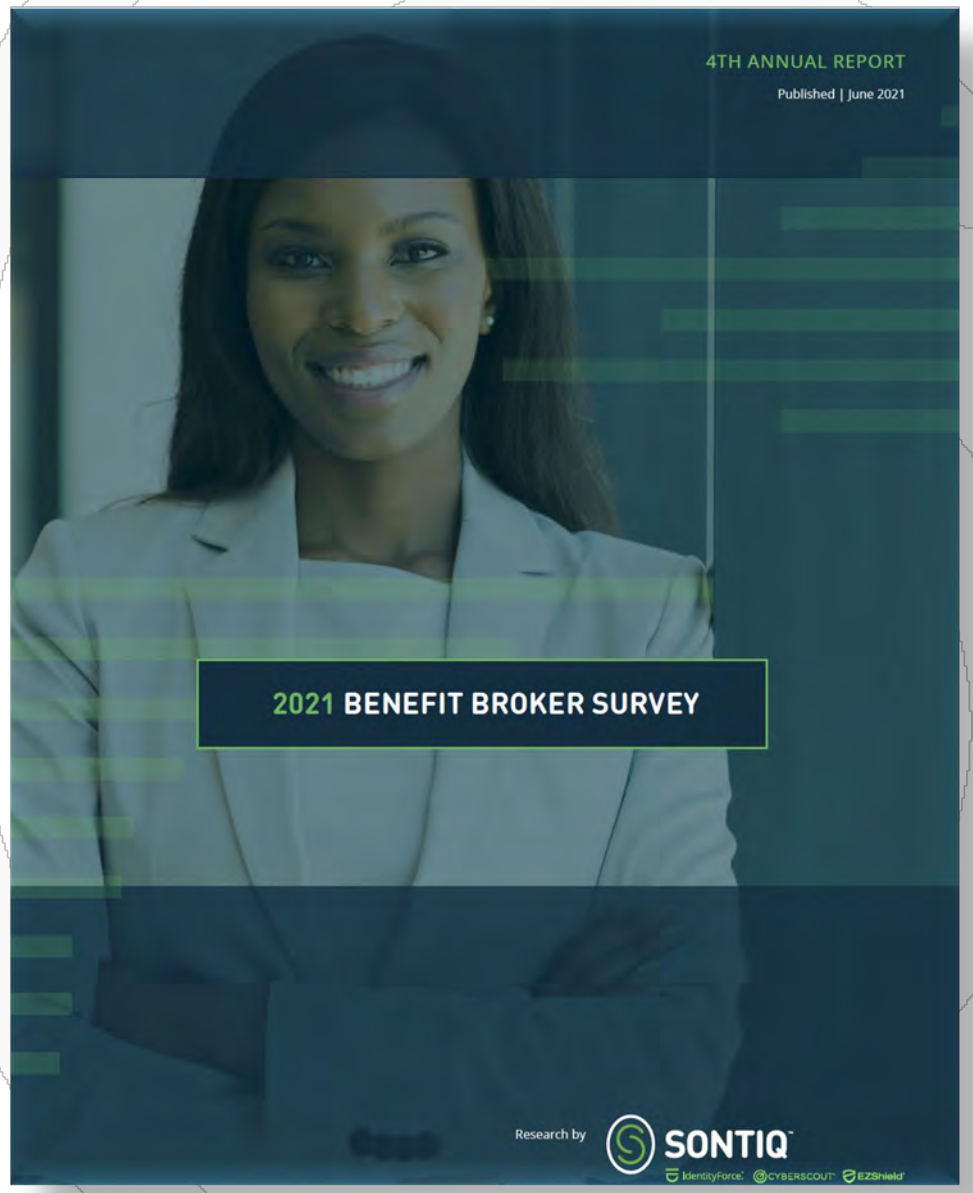
EMPOWERMENT THROUGH EDUCATION

Discover more at
SONTIQ.COM/RESOURCES

webinars@sontiq.com

SONTIQ™

Intelligent identity security.



SONTIQ™

Intelligent identity security.

WITH SONTIQ,
YOU CAN GO ABOUT YOUR
BUSINESS INTELLIGENTLY,
KNOWING THAT THE INDUSTRY'S TOP BRANDS ARE WORKING FOR YOU.

THANK YOU

Wishing you good health.

webinars@sontiq.com

CONFIDENTIALITY NOTICE

This Presentation ("Presentation") has been prepared by or on behalf of Sontiq, Inc. and/or its affiliated companies ("Sontiq") for the purpose of setting out certain confidential information regarding Sontiq's business activities, plans and strategy. References to "Presentation" include any information which has been or may be supplied in writing or orally by or on behalf of Sontiq in connection with the Presentation or in response to any follow-up inquiries from the Presentation.

This Presentation and the information contained herein are confidential. In addition to the terms of any confidentiality agreement you may sign with Sontiq, by viewing the Presentation, you agree that you and each of your agents, representatives, advisors, directors or employees (collectively, "Representatives") will not, and will not permit any third party to, copy, reproduce or distribute to others this Presentation, in whole or in part, at any time without the prior written consent of Sontiq, and that you and all Representatives will keep confidential all information contained herein not already in the public domain and will use this Presentation for the sole purpose of familiarizing yourself with certain limited background information concerning Sontiq and its business strategy, plans and activities. If you have signed a confidentiality agreement with Sontiq, this Presentation constitutes Confidential Information for the purposes of such agreement. If you do not agree to the terms of this Notice, you may NOT view, copy or distribute this Presentation.

While the information contained in this Presentation is believed to be accurate, Sontiq has not conducted any investigation with respect to such information. Sontiq expressly disclaims any and all liability for representations or warranties, expressed or implied, contained in, or for omissions from, this Presentation or any other written or oral communication transmitted to any interested party in connection with this Presentation, so far as is permitted by law.

No representation or warranty is given as to the achievement or reasonableness of, and no reliance should be placed on, any projections, estimates, forecasts, analyses or forward-looking statements contained in this Presentation which involve by their nature a number of risks, uncertainties or assumptions that could cause actual results or events to differ materially from those expressed or implied in this Presentation. Except to the extent otherwise indicated, this Presentation presents information as of the date hereof. The delivery of this Presentation shall not, under any circumstances, create any implication that there will be no change in the affairs of Sontiq after the date hereof. In furnishing this Presentation, Sontiq reserves the right to amend or replace this Presentation at any time and undertakes no obligation to update any of the information contained in the Presentation or to correct any inaccuracies that may become apparent.

This Presentation shall remain the property of Sontiq. Sontiq may, at any time, request that you and/or your Representatives promptly deliver to Sontiq or, if directed in writing by Sontiq, destroy all confidential information relating to this Presentation received in written, electronic or other tangible form whatsoever, including without limitation all copies, reproductions, computer diskettes or written materials which contain such confidential information. At such time, all other notes, analyses or compilations constituting or containing confidential information in your or your Representatives', possession shall be destroyed. You may be required to certify such destruction to Sontiq in writing.

This Presentation contains information that is proprietary and confidential to Sontiq, its partners, vendors and/or clients, and is intended only for the use of authorized individuals or entities. Any unauthorized use, dissemination, distribution or copying of this Presentation is strictly prohibited and any breach of this provision may result in civil and/or criminal action being taken against you.