DATA PROTECTION:

Employer Obligations and Motivations

ITRC IDENTITY THEFT RESOURCE CENTER

GENERALI GLOBAL ASSISTANCE

PRESIDENT & COO, GLOBAL IDENTITY & DIGITAL PROTECTION SERVICES
GENERALI GLOBAL ASSISTANCE (GGA)
Paige L. Schaffer

PRESIDENT & CEO
IDENTITY THEFT RESOURCE CENTER (ITRC)
Eva Velasquez

CONTRIBUTORS
Nikki Fiorentino, ITRC
Kelly Dwyer, ITRC
Alex Hamilton, ITRC
Karen Barney, ITRC
Megan Dwoskin, GGA

CONTACT
Eugenia Buggs
VP, Global Marketing, Identity Protection Services
Generali Global Assistance
4330 East West Hwy, Suite 1000
Bethesda, MD 20814
240-330-1091
eugenia.buggs@us.generaliglobalassistance.com

EXECUTIVE SUMMARY

Data breaches are not a new concern for businesses, as they have long known the havoc that one can exact upon them. With 2017 on pace to reach an all-time high of nearly 1,500 data breaches reported[1], businesses need to be more prepared than ever to deal with the near certainty that they will be targeted for a data breach. In order to mitigate their cybersecurity risks, it is important for employers to not only recognize the importance of protecting their customers' personally identifiable information (PII), but their employees' PII as well.

In this white paper, we explore employers' obligations to protect employee information and best practices for mitigating risk of a data breach. By looking at the types of employee information businesses collect, how data is compromised, current information protection legislation, and best practices for data protection, we paint a more complete picture for businesses to understand all the reasons to protect employee data and offer a comprehensive approach for how businesses can take a more proactive role in protecting it.

How is your company protecting employee data?

What Types of Data Should Be Protected?

In order for businesses to build best practices for the protection of employee data, they must first understand the different categories of employee data they collect. Then they can organize it and implement strategies to protect the data accordingly. The three types of employee data that businesses must protect are personal, financial, and medical. These are further broken down into three types of identifying information based on the level of sensitivity associated with the information and federal regulations—PII, SPII, and PHI.

Personally Identifiable Information (PII)

PII is defined as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[2]

Sensitive Personally Identifying Information (SPII)

SPII is defined as "personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual."[3] For many employers, this means protecting an employee's SSN, banking information, and contact information (such as email, home address, phone number, etc.).

Personal Health Information (PHI)

Employers also need to be cognizant of protecting PHI. For most employers, PHI will include medical information that has been, often inadvertently, shared with them by employees, insurers or medical professionals. A related data type, that PHI is often mentioned in conjunction with, is HIPAA information.

HIPAA, or the Health Insurance Portability and Accountability Act of 1996, is legislation that provides data privacy and security provisions for safeguarding medical information. Oftentimes medical data about individuals is referred to as “HIPAA data” because of the assumed protections that apply to its safeguarding. However, while some of the PHI employers receive is often the same data that HIPAA regulations apply to when it’s shared with a medical provider or insurer, it is important to note that HIPAA legal protection standards do not apply to this same data when it is shared with most employers.[4]

Anonymized Data

Another data type that employers should consider protecting is anonymized data, which is information that has been sanitized in an effort to make it seemingly impossible to extract potentially sensitive information from the dataset, and often includes seemingly de-identified PII and PHI information.

Anonymized data is a type of information not always considered sensitive enough to protect. However, with advances in the ability to reidentify this data type—opening the door to use it for harmful purposes—it’s important that employers consider protecting it as well. Employers need to look no further than this data type’s origin for an explanation as to why it’s so often overlooked as potentially sensitive data. The process of anonymizing data was originally adopted from the field of microdata collection for use in the protection of financial and personal information. One prominent example of such anonymized microdata, which has been in use for decades, is the collection of census data. While the collection of this is important in every industry from public health to financial services, the risk of an invasion of privacy was present.

This is not unlike the risk to employers when the HR department collects census-like “public” information from employees such as gender or ethnicity. To protect against this risk, microdata collectors anonymized the data. In other words, such data points as names, locations and other sensitive personal attributes were removed or

reconfigured to prevent a link between the data source and its related data.[5]

The removal or severe alteration of sensitive or personal data would help protect the data and its subject, which is why organizations often don't consider this type of employee data as a set that needs to be protected beyond the anonymization process; however, this technique is not fool-proof. Researchers have found that anonymous data is not as anonymized as one would think. There is a risk that data that has been anonymized can be "reidentified." As early as 2000, a researcher found that 87 percent of Americans could be uniquely identified using only their birthdate, gender, and zip code.[6] This researcher, a Harvard professor, recently reidentified anonymous volunteers in a DNA study, which included information about sensitive health records and other data.[7] She did so using the same three identifiers, which are not often considered PII, let alone SPII. While a company can hope that no one ever attempts to reidentify their anonymized employee data, it should be understood that even this sanitized data holds valuable information. Therefore, it is important for companies to recognize that data anonymization is not a remedy for protecting employee data, and that leaving even anonymized data unprotected increases risk.

Of course, while companies should take steps to guard all personal information, not all personal information is equal in value. The value of the information taken in a breach is determined by how much someone can gain from it. The more reach a thief has with a particular data asset, the more damage can be done—thus the more value it can carry. It's easy to understand why an email address or phone number is less valuable than a SSN. This is why it is so important for companies to realize that protection of employee data is just as important as protection of customer data.

Why Employers Should Protect Employee Data

While this paper is not meant to serve as any form of legal advice, it is important to introduce some of the legislation that has been developed to protect the data of employees. Here, we review the history and the underlying foundations which make up the laws. Currently, there is no federal legislation regulating data breach notifications in regard to employee data. Legislation regulating the protection of employee data is far more active on the state level.

Since 2002, when California enacted the first state data breach notification law, 47 other states have passed their own statutes, as well as Washington D.C., Guam, Puerto Rico, and the Virgin Islands. State breach notification laws, for the most part, are outlined in a similar manner. They include information on exactly who is under obligation to comply with the law; the definition of PII and "security breach;" benchmarks for harm in order for notification to be necessary; notification requirements; and how the law will be enforced and by whom.

It is interesting to note that most data breach notification laws, when enacted, typically addressed only the collection of PII in electronic format. This was, of course, problematic, as many breaches would go unreported if low-tech methods of exposure were involved. As of now, 10 states include reported breaches involving both electronic and paper formats.

Two areas in which state laws typically differ are in the definition of PII and the level of harm that triggers a notification. Over the years, more and more states have added medical and/or health insurance information to their definitions of PII.

Most recently, a handful of states have amended their laws to include usernames and email addresses when they are breached with an

associated password or security question. The underlying reasoning is that this information could give someone access to an individual's online accounts.

Another area in which state notification laws differ is in the benchmark that must be met in order for notification to be mandatory. For some, any unauthorized access to personal information would trigger the need for a notification, while in others a risk assessment should first be conducted to measure the risk of harm from the access and/or misuse. Companies in each state should be aware and knowledgeable of the data breach notification requirements in their state. This should be in addition to understanding any federal regulations they are held to, and how these two levels of statutes engage with each other.

Most data breach notification laws, when enacted, typically addressed only the collection of PII in electronic format.

The PHI that employers collect may not be specifically protected by HIPAA, unless the employer is a covered entity,[8] but it is in the best interest of a company to operate as if it is. Health information can be used inappropriately in myriad ways if it should fall into the wrong hands. The repercussions of this could range from an employee being upset about their coworkers knowing about their health condition, all the way to discrimination lawsuits brought forward for hiring practices. So, while most companies will not be regulated or audited for HIPAA compliance regarding the collection or sharing of PHI, they should consider following best practices in regard to their custodianship of employee PHI.

Besides legal responsibilities, businesses and organizations should respect their employees enough to protect them. No one wants their employees to be miserable, but it is even worse that the victimized employee is miserable because their company did not protect them from a crime. When employees are faced with identity theft—just as when any individual becomes a victim—there are notable consequences. Victims may experience a sense of mistrust, feelings of frustration, and an understandable level of paranoia wondering what will happen next. All of this can take a toll on their productivity at work, which includes missing time from their job in order to resolve their identity theft issues.[9] The latest Identity Theft: The Aftermath report found that 55 percent of identity theft victims surveyed had to take time off of work to deal with the issue. The respondents reported a loss of income due to both the theft and their missed work hours. Victims also reported issues resulting from their identity theft that led to "presenteeism," which happens when a victim shows up for work but is busy trying to connect with financial institutions, law enforcement, and other entities.[10] These victims also cited physical and psychological issues such as an inability to concentrate (39 percent), sleep disturbances (42 percent), rage or anger (58 percent), and a loss of ability to trust (51 percent).[11] These issues, among others, ultimately affect the employees' ability to be productive in the workplace.

Business Malware

In January of 2017, a business' computer system was attacked by an unknown individual using ransomware software. Even though their anti-virus software stopped the attack, the individual was still able to access a server which contained employees' driver's license numbers, Social Security numbers, health insurance numbers, names, and date of birth among other PII. Immediately upon learning of the attack, the company initiated an investigation with a forensic firm. They also set to work and quickly removed the affected server from their systems, switched to a back-up system, and reset passwords companywide. Following the event, they also updated and strengthened their security systems.

Trends in Data Breaches: How Your Company's Data Can Be Compromised

Data is being compromised in an ever-growing number of ways, including, but not limited to, hacking, spearphishing, and accidental internet exposure. The Identity Theft Resource Center (ITRC) has been tracking data breaches since 2005 as part of their mission to educate and assist victims of identity theft. Along with the number of data breaches being reported, the ITRC's Data Breach Report breaks these events down by industry, number of records, type of information included in the breach, and how the information was compromised. This data allows us to understand data breach trends and assess risks accordingly. So far in 2017, hacking accounts for the large majority of data breaches.

Year to date, the ITRC has tracked 791 data breach incidents, with two thirds of those (63.3 percent) being attributed to hacking attacks.[12] Furthermore, spearphishing as a method of hacking is becoming an increasingly serious issue. Nearly half of all hacking incidents identified on the ITRC's data breach list have involved spearphishing. Spearphishing uses targeted emails that are designed to lure an employee or manager into providing various types of personal information, such as tax or payroll information. These emails are more dangerous than the usual phishing emails in that they are highly specific to the recipient and usually appear to come from a legitimate and trusted source.

Data breach attacks may also use malware to gain access to information. One such type of malware is ransomware which, once downloaded, compromises a company's computer systems and extorts the company to regain access or control to their systems and data. Of course, malware is also used to steal information.

One case that companies should be paying attention to is the recent WannaCry ransomware attacks. In one of the largest malware attacks in history, it brought businesses all over the world to a screeching halt. The malware, which was able to attack computer systems running an older version of Windows, encrypted the businesses' data and then held it for ransom.[13] There was a wide range of industries that were attacked, but notable targets included the British National Health Service,where their doctors were locked out of patient files and they had to send patients to other hospitals;[14] FedEx, which admitted the ransomware had caused disruptions in its service;[15] and French auto-maker, Renault, was forced to stop production at its plants.[1617] The WannaCry attack showed the world, and the businesses within it, how vulnerable we are to security threats that can cripple our infrastructure.

WannaCry Ransomware

In May of 2017, hundreds of thousands of computers, in 150 countries were infected with the WannaCry ransomware. The ransomware infected these computers, encrypted the data on its network, and then demanded that a ransom be paid in order to get the information back. Computer networks that were infected included high-level targets such as Nissan Motor Company, Spain's Telefonica, and Deutsche Bank, among others.

The use of work computers for personal use also puts companies at risk of having data stolen or breached. This is because company designated email programs most often have a higher level of protection against spam than a personal email would have. Therefore, employees are more likely to end up clicking on a malicious link received in their personal email, which can still devastate the company's IT infrastructure.

While much of the focus these days is on high-tech cybercrimes, there are still plenty of low-tech ways to steal data. The reality is that a company is just as likely to suffer a devastating data breach due to sensitive paperwork that was accidentally discarded without being destroyed or shared with unauthorized third-parties or documents getting lost in the mail, as they are to cyberattacks. While all of these examples are innocent enough, they can still potentially expose employees' records to unauthorized people. The result of that mistake can cost a company a lot of money in notification letters, a loss of community trust, and damage to their employee relations.

Workplace Spearphishing

In February 2017, a university discovered that an employee was the target of a spearphishing attack. The employee received an email purporting to be from an executive, requesting copies of employee W-2 wage and tax statements. In response to that email, a spreadsheet of employee W-2 information was sent to an unauthorized email address. The spreadsheet reportedly contained names, addresses, Social Security numbers, and wages and tax information for the University's employees from 2016. Following the notification of the breach, the University revised their policy and procedures regarding the handling of personal information and began conducting additional training and education.

Best Practices in Protecting Employee Data

Knowing how employee data is compromised creates a good foundation for protecting that data. While there are IT best practices that would be far outside the scope of this paper, companies can start by laying the groundwork for a solid program by applying some standard best practices. These include using strong encryption processes, creating a culture of cybersecurity, proper custodianship of data, and vetting of third-party vendors.

Encryption

Encryption should be standard practice for companies aiming to protect their employees' data. However, though many companies will focus on encrypting customers' PII or intellectual property, not as many are using the same level of security for their own employee data. A recent Sophos survey of 1700 IT decision makers found that only 57 percent of their companies encrypted their HR files, but 76 percent encrypted their customers' data.[18] This is problematic as employee data can be far more valuable than customer data. While a company is less likely to have their customers' SSNs in their database, they will have those of their employees. The amount and type of data held on employees make it a much more attractive target for hackers or thieves, and yet this information is often left vulnerable.

Creating a Culture of Cybersecurity

Most often, the weakest link in a company's security are human beings. No matter what security protocols or protections a business has in place, all it takes is one employee to click on the wrong link to potentially put your system, and the data within it, into the hands of hackers. That being said, companies can strengthen measures against human error by creating a culture of cybersecurity within the workplace. This should be created just like any other type of corporate culture, where management guides the reinforcement of values among employees.

In this case, the value is keeping data safe and secure. In fact, having upper level management active in practicing good cybersecurity habits has an added benefit. High-level executives have become a targeted population for phishing attempts due to their ability to access information companywide. The FBI says that companies who become victims of this type of fraud are estimated to lose between $25,000 and $75,000 each and that companies nationwide lost $2.3 billion from 2014-2016.[19]

Of course, C-level employees are not the only targets of such phishing attempts. Cybersecurity should not be an afterthought for employees, but a top priority. Employees must be educated on the risks of unsafe practices and be encouraged to engage in discussions about security risks. Creating such an environment can be done by holding educational lunches, posting relevant information around the office, and/or sending regular emails with security tips. It may also be helpful to create measurable goals and share the results with your company.[20]

Companies should also consider demonstrating their commitment to protecting the data of their employees by offering an identity protection service as a voluntary or employer-paid benefit.

Accidental Data Exposure

In February of 2017, a college student unintentionally gained access online to a file containing information about the school's students. After the student immediately notified the College, it removed the files, which had been accidently included in another file the College had uploaded. The files contained students' Social Security numbers, names, addresses, and identification numbers. Following the situation, the college did a thorough search of their entire server to look for other erroneously placed files and put in place a mandatory practice of reviewing all files prior to uploading them.

An added bonus of offering an identity protection service is that many include resource libraries with content that can help educate employees on cyber safety best practices, as well as send periodic identity protection status emails that assist in keeping cybersecurity at the top of employees' minds.

Additionally, companies should consider periodically sharing free information to minimize risks of identity theft and mitigation resources from reputable consumer advocacy organizations, such as the ITRC and Federal Trade Commission.

Empowering Your Employees to Practice Good Data Custodianship

Being a good custodian of employee data is crucial in avoiding a data breach. This includes proper collection, handling, tracking, and sharing of information. When it comes to handling and tracking this information, it is important to remember exactly what information you collect. Evaluate your intake forms (for both employees and customers) and assess your company's need for requesting certain pieces of PII. If your company does not need a specific piece of PII, don't collect it. Once data is collected, catalogue it and identify all the places where that information is stored throughout the company's networks. Once this process is completed, determine who within the organization needs access to that information. Tiered permissions may be necessary as you develop an Authorized Use Policy, detailing who can see, access, and modify information.

In addition, strong storage protocols should be well defined when it comes to protecting the security and privacy of all pieces of PII. Again, this is based on the types of information being collected and where it is located within the organization. For example, one best practice is to create different files for different types of employee information. This means creating separate files for employee health information, PII, and SPII. These files should be kept in a different location than the employees' basic HR file and only available to those who would need access to such information. This will create a safeguard against the exposure of information which may create issues if used inappropriately.

Employers should also be cognizant about the format in which files are stored so that they can best create safe storage practices. Is the information being stored electronically? Does it need to be encrypted? Are there hard copies? Is it stored physically onsite, offsite, or in the cloud? All of these issues need to be addressed in your data protection procedures and policies.

If your company doesn't need a specific piece of PII, don't collect it.

The sharing of information internally is also something which should be addressed and standard operating procedures (SOP) should be created. These procedures should ensure that only information that needs to be shared is included in shared files. SOPs should also ensure that employees within the company know how to safely transmit employee data whether that be physical transportation of a file to another office or the emailing of data within the company. Employees should know how to handle this information once they have received it, how long they should have access to it, and how to return or dispose of it once they have completed the necessary task. A good place to start with education is in management. While employees should be sharing any sensitive data they are required to provide their company with only HR, it is still commonplace in many organizations that employees sometimes send this information to the managers they report to, whether that be detailed information regarding a health issue which kept them from attending work one day or a change of address. Although these practices need to start at the top with management and executives, the entire company should be aware of them in order to create a culture of security.

Vetting Third-Party Vendors
An often overlooked best practice is vetting third-party vendors who have access to your employees' PII.

While companies might have working processes in place for safeguarding employee data, vendors are often the gateway to leaked information falling into the wrong hands. In recent years, 63 percent of breaches were traced to third-party vendors.[21]

This staggering statistic is not only unfortunate but also can be quite costly for businesses. For example, approximately $10 million on average is spent annually to respond to security incidents, in addition to reputation loss, brand damage, theft of assets, and loss of worker productivity.[22]

The first step in vetting a vendor is to look at their own security practices and make sure they perform data back-ups, recoveries, and internal security audits regularly. They should also have redundant back-up servers. In addition, the vendor should have a business continuity plan in place, which is also regularly reviewed and updated. Companies should also ensure that third-party vendors run background checks on their employees.[23] Third-party vendors that are vetted should include both suppliers and employee benefits providers. Once again, a company's data protection is only as strong as its weakest link. Vetting third-party vendors will help ensure that companies are not blindsided by a vulnerability that they did not even consider.

Third-Party Business Hacking

In December of 2016, a company was alerted by its hosting system that their website had to be taken offline. In an investigation into why the website was taken offline, the company found that their website had been built by a third-party vendor who had installed malware to collect the credit card information of the customers purchasing items online. Once they learned about the malware, the company hired a forensic investigation firm to further review the malware installation and identify which customers' payment information had been compromised. The forensic firm then did a review of the website to ensure it was safe and the company implemented stronger security protocols.

Conclusion and Key Takeaways

In cybersecurity, the only certainty is change. Individuals and businesses alike must be able to adapt and stay abreast in the ever-evolving threat arena. There are legal and ethical practices that every business should adhere to.These include assessing the information they gather on their employees, establishing guidelines for who can retrieve that information and how it will be stored, and making crucial decisions about putting employees' data security at the top of their priority lists.

Moreover, in this age of connectivity, businesses must hold their outside connections to high standards for security. This includes the aforementioned third-party vendors, including suppliers and benefits providers, who have direct access to the company's network and/or data. Even something as simple as an email exchange from a compromised vendor account can lead to malware infections.

Finally, all cybersecurity your company engages in starts with your employees. Technology that is designed to protect your network cannot compete with an untrained workforce that is not up-to-date on both the latest threats and best practices. Keep your workforce informed, and help them protect their own data from a breach.

References

(1) Identity Theft Resource Center (ITRC). (2017, May 9). ITRC Data Breach Report. Retrieved from http://www.idtheftcenter.org/images/breach/2017Breaches/ITRCBreachReport2017.pdf

(2) McCallister, E., Grance, T., & Kent, K. (2010, April). Guide to Protecting the Confidentiality of Personally Identifiable Information (National Institute of Standards and Technology (NIST)). Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

(3) Department of Homeland Security (DHS). (2012, March). Handbook for Safeguarding Sensitive PII. Retrieved from https://www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguardingsensitivePII_march_2012_webversion.pdf

(4) U.S. Department of Health & Human Services (2017, June 16). “Employers and Health Information in the Workplace”. Retrieved from https://www.hhs.gov/hipaa/for-individuals/employers-health-information-workplace/index.html

(5) Coull, S. E., Monrose, F., Reiter, M. K., & Bailey, M. (2009, March). “The challenges of effectively anonymizing network data”. Retrieved from https://pdfs.semanticscholar.org/d2cc/316ff7b651640140a17b340d8157f1faf3b7.pdf

(6) Anderson, N. (2009, September 08). ““Anonymized” data really isn’t—and here’s why not.” Retrieved from https://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/

(7) Tanner, A. (2013, April 25). “Harvard Professor Re-Identifies Anonymous Volunteers In DNA Study”. Retrieved from https://www.forbes.com/sites/adamtanner/2013/04/25/harvard-professor-re-identifies-anonymous-volunteers-in-dna-study/#780b343d92c9

(8) US Department of Health and Human Services. (n.d.). “HIPAA Privacy Rule and Its Impacts on Research”. Retrieved from https://privacyruleandresearch.nih.gov/pr_06.asp

(9) Identity Theft Resource Center (ITRC). (2016, October 17). Identity Theft: The Aftermath (Rep.). Retrieved from http://www.idtheftcenter.org/images/page-docs/AftermathFinal_2016.pdf. 9.

(10) Ibid.

(11) Ibid. 18-20.

(12) As of July 7, 2017

(13) Ng, Alfred. (2017, May 15). WannaCry ransomware loses its kill switch, so watch out. Retrieved from https://www.cnet.com/news/wannacry-ransomware-patched-updated-virus-kill-switch/

(14) Donaldson, S. (2017, May 19). WannaCry Ransomware: Who It Affected and Why It Matters – RHD Blog. Retrieved from https://developers.redhat.com/blog/2017/05/19/wannacry-ransomware-who-it-affected-and-why-it-matters/

(15) Vigliarolo, B. (2017, May 19). 10 major organizations affected by the WannaCry ransomware attack. Retrieved from http://www.techrepublic.com/pictures/gallery-10-major-organizations-affected-by-the-wannacry-ransomware-attack/10/

(16) Figurelli, A. (2017, May 16). Mitchell International, Nissan Among Companies Affected by WannaCry Global Ransomware Attack. Retrieved from http://www.repairerdrivennews.com/2017/05/16/mitchell-international-nissan-among-companies-affected-by-wannacry-global-ransomware-attack/

(17) Whitmore, W. (2017, July 05). How Similar Are WannaCry And Petya Ransomware? Retrieved from https://www.forbes.com/sites/quora/2017/07/05/how-similar-are-wannacry-and-petya-ransomware/#78e7f78546eb

(18) Zorabedian, J. (2016, January 19). Survey Shows Many Businesses aren't Encrypting Private Employee Data. Retrieved from https://nakedsecurity.sophos.com/2016/01/19/survey-shows-many-businesses-arent-encrypting-private-employee-data/

(19) Krebs, B. (2016, April 7). FBI: $2.3 Billion Lost to CEO Email Scams. Retrieved July 07, 2017, from https://krebsonsecurity.com/2016/04/fbi-2-3-billion-lost-to-ceo-email-scams/

(20) McKerchar, R. (2015, October 09). Practical IT: How to create a culture of cybersecurity at work. Retrieved from https://nakedsecurity.sophos.com/2015/10/09/practical-it-how-to-create-a-culture-of-cybersecurity-at-work/

(21) Hughes, C. (2016, December 07). Why third party cybersecurity matters. Retrieved from http://www.csoonline.com/article/3142738/network-security/why-third-party-cybersecurity-matters.html

(22) Miller, C. (2016, May 2). How To Succeed At Third-Party Cyber Risk Management: 10 Steps. Retrieved from http://www.darkreading.com/operations/how-to-succeed-at-third-party-cyber-risk-management-10-steps/a/d-id/1325342

(23) Bailey, T. (n.d.). Managing Third-Party Vendor Risk. Retrieved from https://identity.utexas.edu/id-perspectives/managing-third-party-vendor-risk

Founded in 1999, the Identity Theft Resource Center® (ITRC) is a nationally recognized non-profit organization established to support victims of identity theft in resolving their cases, and to broaden public education and awareness in the understanding of identity theft, data breaches, cybersecurity, scams/fraud, and privacy issues.

The ITRC provides no cost victim assistance and consumer education through its call center, website, social media channels, live chat feature, and ID Theft Help Mobile App.

www.idtheftcenter.org

Generali Global Assistance (GGA), proudly owned by Europ Assitsance Holding and part of the multinational Generali Group, has been busy protecting clients and their customers for over 50 years–via co-branded services and behind the scenes as a white-labeled provider. GGA was one of the first companies to provide identity theft resolution services in the United States. They are the identity protection engine behind some of the biggest names in the Fortune 500, and today are a leading provider, proudly protecting millions of lives from the growing threat of identity theft. Their comprehensive identity protection is a powerful combination of credit monitoring and alerts, advanced identity monitoring technology, online data protectoin tools, and award-winning resolution.

For more information about preventing identity theft for your employees, customers, or members, contact Generali Global Assistance Identity Protection Services at

us.generaliglobalassistance.com/identity-protection


ITRC
IDENTITY THEFT
RESOURCE CENTER


GENERALI
GLOBAL ASSISTANCE