HOW SAFE IS YOUR DATA?

PROTECTING SENSITIVE INFORMATION IN YOUR FIRM'S PRENEED TRUST.

BY BILL WILLIAMS

We live in a digital world where cyberattacks are commonplace and our private information is constantly vulnerable. Recent Equifax breaches, which exposed the data of more than 145 million people (at least one person in every U.S. family, it's estimated), certainly drove that point home. But while we often take steps to secure our personal information from these dangers, many of us overlook the importance of protecting other sensitive data, such as the financial information of a deathcare firm's trust. And with so much at stake, the consequences of insecure data are severe.

Consider this: Your preneed trust is your future; it's what will sustain your firm in perpetuity. But what if a data breach happens and an outside threat accesses the sensitive information in your trust? Funds could be stolen and private client information captured and shared. You could lose the strong reputation you've built with your clients, and worse, all you've invested into your business.

Fortunately, there are practices you can put in place to protect the financial information of your firm's preneed trust. Regular monitoring and audits of your account, adhering to PCI compliance, implementing email security and backing up your data are just the beginning. Dive in below to learn more about securing your trust fund data.

Monitoring Accounts

Just like your bank account, you should check the status of your trust as often as possible. Keeping an eye on it will help you know when something is wrong; otherwise, your blissful ignorance could result in devastating consequences. If you are working with a third party that provides reporting on your trust, be sure to take advantage of these reports by reviewing them on a regular basis. You should choose a partner that enables you to check your trust's balances proactively, track your receivables and earnings down to the contract level and access monthly statements immediately.

Staying engaged with the activity and transactions of your trust is your first line of defense against potential data security breaches. It will educate you about your business' finances and allow you to spot any warning signs with time to adjust and prevent a crisis. Of course, your trust team, if you have one, will have your trust's finances under control, but it is still your money and I always recommend that you keep it top of mind, too.

Regular Account Audits

When you work with financial data and sensitive information such as in a preneed trust, ensuring the safety and validity of your accounts is not optional. Another way to spot warning signs with your trust is through regular internal audits, which is an important risk management best practice often overlooked. Nobody wants to spend precious time gathering and providing files of information while everyday duties and responsibilities pile up, but when a regulatory review comes, you'll be prepared. Regular account audits will

beef up the security of your accounts, and they're an invaluable tactic to discover your trust's inefficiencies or areas for improvement.

Still think you don't have the time or the necessary background to properly audit your trust's accounts? Working with a third party that specializes in trust recordkeeping is an easy way to take this burden off your shoulders. When choosing a partner, make sure they adhere to SSAE-16 Type II auditing compliance. This will ensure that your accounts are being managed according to the strictest auditing standards to keep your data safe and secure.

Payment Card Industry Compliance

Can your clients pay by credit or debit card? If so, you must adhere to Payment Card Industry (PCI) compliance. The purpose of PCI compliance is to prevent, detect and react to potential breaches or hacks that could threaten payment card data and result in costly fraud. If you run a small business, you might think you're immune to these types of attacks, but attackers often focus on small businesses as they are less likely to implement security measures and are therefore more likely to be vulnerable. Don't let yourself fall into this trap!

Start by following guidance from PCI Security Standards to help keep your cyberdefenses primed against attacks aimed at stealing cardholder data. According to the PCI Security Standards, there are 12 PCI-compliant requirements that meet a variety of security goals. They include maintaining a firewall configuration to protect cardholder data, using and regularly updating anti-virus software and creating unique software passwords. If you choose a data-hosting provider to take care of this for you, ask for documentation that PCI compliance requirements are met.

Email Security

Since the advent of email, criminals have been using it to their advantage, spreading malware, spam and phishing attacks and using deceptive messages to entice recipients to download viruses. The sensitive information contained in emails or about email accounts is also at risk. For example, in 2013, a historic data breach at Yahoo affected every single customer at that time – three billion accounts. Names, email addresses and passwords were stolen and later were found being sold on the dark web.

To protect yourself and your trust's important data from these risks, conduct all trust-related communications via a secured system. Using a dedicated system rather than a traditional email account keeps your messages private and shields you from security threats. It's also important for you and your staff to spot red flags when opening emails, such as misspellings, offers that seem too good to be true or messages that instruct you to open an attachment. It might seem like common sense, but only click links or open attachments from sources you know and trust. Otherwise, you could unwittingly install malware on your own device, opening up your entire network to threats. Even in our digital age, human error can lead to data breaches and human savvy can prevent them.

Preserving Your Data

Now that you know how to protect your data from attacks and outside threats, you must also take steps to preserve your data. What happens if your equipment malfunctions or is damaged? For instance, what if flooding irreparably destroys your systems or files – how will you recover your preneed trust's information? In cases like these, storing files on a cloud system will protect you from losing valuable data. Using a cloud system also adds convenience, allowing you to access your information from any device, whether you're at home or on the road.

Of course, there are security vulnerabilities with the cloud, especially if you're not taking proper safety precautions. Start by choosing a provider with an encrypted cloud service, which will make it difficult for any would-be attackers to break in. Your cloud data should also be password protected, and you'll need to choose a strong, unique password. You also need to make sure that wherever you log on, you are using a secure network you trust. That means you should not use free Wi-Fi networks when accessing trust information outside the office. Those networks are open to the public and present much higher risk than your secure office network.

Another way to preserve your data is by regularly saving it to an external hard drive. External and portable hard drives connect to one computer at a time and usually do not have wireless capabilities, meaning the device must be plugged into a computer to access its data. Because of this, external hard drives make your data less accessible than when stored in a cloud system, and they are easy to use, less vulnerable to attack and offer the option to schedule regular backups.

Your Data Is as Safe as You Make It

If you've never considered protecting your trust's sensitive data before, now is the time to start. You simply can't take any risks when you hold the future of your business in your hands. In addition to preserving your own investments, your clients are depending on you to protect their personal information and funds as well. With everything to lose, your trust requires the best security possible.

I'm offering these suggestions because these are the security measures we implement at my own company, Funeral Services Inc. As a licensed funeral director myself, I understand how these security challenges can threaten your business and clients. That's why it's important to me that FSI offers solutions that can protect preneed trusts, and I'm proud to say we are the only known deathcare trust recordkeeper in the United States that uses highly secure software and procedures and maintains SSAE-16 Type II compliance and PCI compliance to assist in protecting our clients from potential threats.

You can't predict when or if a cyberattack will happen, and no one can prevent all hacks. But you can be ready to face the worst if you have prepared with best practices. By taking the proper steps to protect the sensitive information in your trust, you will ensure your clients' trust and the security of your business' investments.

Bill Williams is president and CEO of Funeral Services Inc.