withum

CYBERSECURITY FOR THE DEATH CARE INDUSTRY

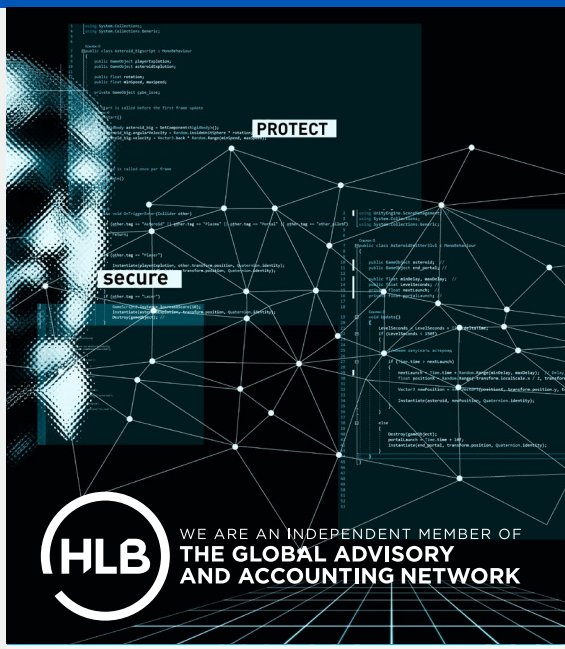
Did you know cyber criminals target the deceased identity data?

"Ghosting" is when a deceased individual's personal information is used to commit fraudulent acts such as account takeovers, social engineering, tax refund fraud, medical identity theft, driver's license identity theft, credit card fraud, and much more.

Just because someone has passed away does not mean they are not susceptible to fraud or identity theft. Personal Identifiable Information (PII), such as names, addresses, date of birth, and social security numbers, are valuable for cyber criminals. They know how to broker this information online and on the dark web, as well as perpetrate account takeovers, commit financial fraud, and orchestrate fraud against families, businesses and estates.

IF YOU ARE A BUSINESS OWNER WHO DEALS WITH DECEASED IDENTITY DATA, YOU ARE A TARGET. WITHUM BRINGS INFORMATION SECURITY AND RISK ASSESSMENTS DESIGNED SPECIFICALLY FOR THE DEATH CARE INDUSTRY.

Don't wait for your business to fall victim to an attack. We apply the highest levels of expertise, security, and privacy — matters are kept strictly confidential and potentially legally privileged.



Withum Cyber Team
T (800) 470 0988
D (212) 537 9397
wcyber.info@withum.com

withum

Whether determining your risk and cybersecurity posture before an incident or immediately following one, Withum's Cyber Team can provide your business with the details and support needed to move forward. Protecting your business and your clients' information is vital in today's world, death care included.

Families trust that your business has done the appropriate due diligence to ensure the utmost security controls are in place to protect the information their loved ones have left behind. When your business suffers an information security incident, you have a crisis on your hands. Incidents in death care involve a degree of uncertainty. You may not know its origin — internal or external — attacking revenue systems, intellectual property, PII and client data. An attack on key assets costs more than just money. Operating in an environment in a reckless and/or negligent manner leaves the business susceptible to legal actions, such as civil and class action lawsuits and regulatory violations.

Due diligence on your part requires that you find the underlying cause of the incident and make the necessary and correct decisions. You need a tactical approach, measuring your business risk efficiently and inexpensively, providing quick, expert and unbiased answers. Whether determining your risk and cybersecurity posture before an incident or immediately following one, Withum's Cyber Team can provide your business with the details and support needed to move forward. Protecting your business and your clients' information is vital in today's world, death care included.

Have Confidence in your Information Security Program. Contact Withum's Cyber Team today at (800) 470 0988 or (212) 537 9397 or email us at wcyber.info@withum.com.

Withum Cyber Team
T (800) 470 0988
D (212) 537 9397
wcyber.info@withum.com

withum
ADVISORY TAX AUDIT