

VBiz Data Breach Response Planning, VBiz Notification & ID Theft Services

Description of Benefits for VBiz

VBiz is a cost effective identity theft and data breach response planning solution for your business which can also be extended to your clients as a unique enhancement of services. VBiz provides an unparalleled suite of services to address the increasing dangers of data breach events facing the SMB business market. It incorporates Pre-Data Breach Services designed to help prepare businesses and avoid the avalanche of issues related to the growing risks of cyber threats. The Data Breach Response Planning and VBiz Notification Services within VBiz are critical tools available to you if the unspeakable happens and you, or any of your clients, experiences a data breach event. The 2018 data breach forecast indicates risks are continuing to grow as technology and data mobility continue to expand. These threats make the benefits of VBiz invaluable by serving as the **Ultimate Safety Net** for you and your clients. As a special bonus, VBiz will also serve to defend your employees and their families for any form of ID theft or fraud event they might experience at any time.

Data Breach Planning and Preparedness Tools (Pre-Breach)

The Data Breach Planning and Preparedness Tools are designed to help prepare your employees and your business to avoid the growing risks of cyber threats.

- Cyber Security Resource Portal
- Dark Web Enhanced Domain Monitoring with email and SMS alerts
- Quarterly cyber security and information governance training events
- Quarterly email newsletter with valuable content to keep you current about the changing cyber threat landscape provided by industry experts
- Monthly Trends Update emails of the most recent ID theft and cybersecurity trends

Cyber Security Resource Portal

A wealth of resources for all of your data security, cybersecurity, and data breach response needs.

Included are e-learning, risk assessment tools, state specific surveys, including data breach, data destruction, safeguards and social media privacy laws.

- ✓ Built and maintained by leading privacy and data security attorneys the Jackson Lewis cyber security resource portal empowers users by offering interactive e-learning modules, assessment tools, sample policies, and numerous training resources.
- ✓ Designed for all levels of users, the portal can help your business build and maintain a compliant information security policy.
- ✓ Sample policies are provided to help you generate and tailor policies specific to your business

Enhanced Domain Scanning

The service employs sophisticated search, data mining and data matching technology to detect if your business domain, or any email address associated with your businesses domain, have been compromised.

- ✓ Automatically identifies all known email addresses at a domain that have been included in discovered dark web Breaches.
- ✓ An initial scan report immediately lets your business know if any of your credentials have been found to be exploited on the dark web.
- ✓ 24/7 monitoring then continuously scours the dark web for an alert of any new breached credentials and will provide an instant email and SMS text alerts if compromise is detected.

In the event of a data breach incident

When an information security breach occurs, your business is required to comply with a patchwork of state and federal regulations. It is key that your response to the event is timely and comprehensive to avoid litigation from both regulators and affected victims. VBiz maintains a constant watch on the ever-changing data breach regulatory environment to keep you compliant should you experience an information security incident.

Data breach response and VBiz Notification services: (Post-data breach)

The information you hold about your customers and employees is as good as gold to identity thieves.

A critical service provided within VBiz is immediate access to a highly qualified and experienced data breach attorney. The attorney will guide you through the critical steps of determining your risk exposure, develop a plan to keep your response to the breach legal, and most critically protect any work product they create on your behalf via attorney-client privilege.

VBiz provides a complete breach response planning and VBiz Notification solution with an execution timeline including a careful review of state and federal compliance requirements for up to two (2) Data Breach events per 12 month period. VBiz provides live response 24/7/365 to answer questions, receive reports of a suspected Data Breach Event and recommended critical first steps. A dedicated point of contact will gather information to determine the nature and extent of the Data Breach event and co-ordinate engagement with qualified attorney who will provide an Initial Data Incident Consultation to discuss basic strategies for investigating and responding to the incident, answer questions and develop next steps. The qualified attorney will recommend VBiz Notification letter content to governmental agencies and Affected Consumers based on the circumstances and compliance requirements of the Data Breach event.

Data Breach Response and VBiz Notification Services:

- Dedicated rapid response team
- Highly qualified and experienced data breach attorney to guide you through the critical steps of breach response
- In-depth assessment to determine compliance and VBiz Notification requirements based on the circumstances of the event
- Data breach VBiz Notification response plan designed to meet compliance requirements of state and federal regulations
- Fully Managed Identity Fraud Research, Remediation and Recovery services for victims of a data breach
- Access to forensic experts to guide you through your cyber security data breach response needs
- Optional Services available to Member Business at preferred pricing, include;

Fully Managed ID Theft Recovery Services for up to 5,000 Affected Consumers

Additionally, VBiz includes victim recovery services for an affected group of up to 50,000 compromised records that correlate to customers and employees. The same extensive ID theft recovery services itemized in the employee benefit plan (see below), are also extended to any customers who become victims...or even suspected victims. VBiz also provides one year of TransUnion credit monitoring to the victims of identity fraud at substantially reduced rates. Extension of identity protection services to non-victims is available at reduced rates.

Employee Benefit PLAN

VBiz provides fully managed identity fraud research, remediation and recovery services for up to 25 employees, owners and directors, extending to 3 generations of their family members. A professional Recovery Advocate handles the research, documentation and legwork to resolve both financial and non-financial identity fraud, saving your employees time, money and lost productivity! Today, when employee benefits are being eliminated and reduced, this is a great additional employee benefit for attracting new employees as well as retaining current valuable employees.

If, for any reason, an employee, owner or director or an eligible member of their family is a victim of identity theft within the term of the program, a professional Recovery Advocate will manage the recovery process with a goal to restore their

name and credit to pre-event status. Vero's Service Provider will handle the follow-up, paperwork, and phone calls on their behalf, through a limited power of attorney authorization. Once an identity theft event is reported, the following actions will be taken to manage their recovery by a professional recovery advocate:

- a. They will be assigned a Recovery Advocate, who will work with them to perform the necessary actions to recover their name and credit history.
- b. The Recovery Advocate will immediately send them a Recovery Packet (if applicable) by email, fax or overnight delivery, with a limited power of attorney form, and instructions for immediate action to be taken.
- c. Once the forms in the Recovery Packet are returned, the Recovery Advocate will perform any or all of the following actions:
 - Place fraud alerts at the three major credit bureaus
 - Provide copies of credit reports from all three credit bureaus and review the reports with them to identify fraudulent activity.
 - Assist in completing the official Identity Theft Affidavit from the Federal Trade Commission to establish their rights as a victim.
 - Contact the Social Security Administration, US Postal Service, Department of Motor Vehicles, among others, to reverse any wrongful information, transactions, or misuse of official documentation as applicable to the case.
 - Research and document any fraudulent transactions, false accounts, or contracts signed with creditors, banks, utility companies, leasing agents, medical facilities, etc., and follow up to make sure all wrongful activity is resolved and removed from credit files.
 - Work with local and federal law enforcement to try to stop the criminal(s) that are misusing the employee's name.
- d. At the close of their case, their Recovery Advocate will provide confirmation of their return to pre-identity theft status.
- e. The Recovery Advocate will provide post-recovery follow-up for 12 months as well as initiate 12 months of free TransUnion credit monitoring at no additional cost.
- f. They will have online Access 24x7x365 to their Identity Care Center and the status of their Identity theft case.

How to use your VBiz services:

Contact customer support at 866-647-6220 for information about the VBiz service if you have any questions about the VBiz services or if you believe you have experienced a data breach event.

When VBiz Services Benefits Start

VBiz Benefits begin on the effective date of the VBiz Program Announcement and receipt of the VBiz Notification letter by the Member Company.

When VBiz Services Benefits End

The benefit period for VBiz, including, without limitation, any renewal terms, if applicable, will be when you are no longer a member or elect to cancel your membership

What is a Data Breach event?

A Data Breach event is an unauthorized or unintentional exposure, disclosure, theft or loss of sensitive, personally identifiable information relating to employees, customers, clients or other individuals that is collected, stored or otherwise used by a Member Company.

Most states and the federal government have enacted legislation that dictate how a business must respond in the event of a Data Breach, within what time frame and in what manner, and may require the business to provide notice to government agencies and/or the affected consumers. There can be fines and penalties imposed by these agencies if the business fails to meet these requirements which vary from state to state. In addition, a business can be subject to significant risk of civil litigation and even class action suits from the affected consumers as well as banks and other businesses that may also have been affected by the event.

VBIZ DESCRIPTION OF SERVICES AND TERMS AND CONDITIONS

"Member Company" is defined as a proprietorship, partnership, limited partnership, limited liability company and will be referred to as such throughout this document.

The VBiz program, as described herein, constitutes the services ("**Services**"). The Services are provided by Merchants information Solutions, Inc. as the service provider ("**Service Provider**").

"Account Administrator" is an individual who has been properly authorized by the Member Company to provide information and direction to the Service Provider and authorize transactions on behalf of the Member Company as may be required by the Service Provider to fulfill the Services. The Service Provider will act on behalf of the Member Company only by authorization from an Account Administrator, who will also be required to provide information to the Service Provider necessary to fulfill the Services.

"Affected Consumer" means a natural person identified by a Member Company to the Service Provider in an approved format as having their personally identifying information compromised as a result of a Data Breach event declared by a Member Company and for which Service provider is providing Services.

These **Terms and Conditions** ("Terms and Conditions") apply to all communications between the Member Company and the Account Administrator acting on behalf of the Member Company and for Service Provider, including, without limitation, your access to and use of the website and any information and resources available therein ("Website"), all communications conducted through the Website, and your purchase of the Services as Account Administrator on behalf of the Member Company.

THESE SERVICES ARE PROVIDED FOR INFORMATIONAL PURPOSES ONLY AND NOT FOR THE PURPOSE OF PROVIDING LEGAL ADVICE. Interaction with ACCESS or the Service Provider or use of materials and/or information provided by ACCESS or the Service Provider does not create an attorney-client relationship between ACCESS or the Service Provider and Member Company. **THE MEMBER COMPANY SHOULD OBTAIN THE ADVICE OF LEGAL COUNSEL WITH RESPECT TO THESE ISSUES.** The Service Provider relies on information provided by the Member Company to develop and deliver the Services and inaccuracy in the information provided by the Member Company may result in errors in the Services.

The Website is intended for users who are eighteen (18) years of age or older. The Services are only available to Companies operating within the United States and its territories. The Service Provider will only provide the Services in conjunction with agencies and institutions in the United States, or territories where U.S. law applies ("Territory").

Acceptance of Terms and Conditions

By using the services, as the Account Administrator acting on behalf of the Member Company and for the company's benefit, signify your agreement to be bound by these Terms and Conditions, the Service Provider's Privacy Policy, incorporated herein by reference and available, and all laws and regulations applicable to the Services offered by Service Provider, whether or not you create an account, register as a member or purchase the Services. Service Provider may, in its sole discretion, modify these Terms and Conditions from time to time and such modified Terms and Conditions shall supersede any prior versions of the Terms and Conditions. Your continued use of the Website and/or purchase of the Services on behalf of the Member Company constitute your acceptance of such modifications and your subsequent use of the Website and the Services shall be governed by the latest version of the Terms and Conditions. The Terms and Conditions are effective until terminated by Service Provider. In the event of termination, the Service Provider Intellectual Property,

Disclaimer of Warranty; Limitations of Liability and Indemnification provisions set forth in these Terms and Conditions shall survive. Service Provider will post modifications to the Terms and Conditions on the Website and indicate the date of the most recent modification.

Service Provider shall not be obligated or responsible to provide the Services for any request based on: (i) an act of fraud, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you or by any owner, officer or director of the Member Company; (ii) losses, damages or expenses arising out of any business pursuits; (iii) losses, damages or expenses that were incurred or commenced prior to the effective date of the Services.

Services are only available to Member Companies established under the laws of the United States and its territories and to consumers who are residents of the United States and its territories. Service Provider will only provide Services in conjunction with agencies and institutions in the United States, or territories where U.S. law applies ("Territory").

Eligibility for Services to the Member Company is based on Data Breach events that are discovered or first known to the Member Company and reported to the Service Provider during the benefit period. Data Breach events that are discovered or first known to a Dealer Company prior to their benefit period are not eligible for Services under this Agreement.

Eligibility for Services to Affected Consumers is based on ID Theft events that are discovered or first known to the Affected Consumer and reported to the Service Provider during the benefit period and within one year from the date the Affected Consumer is identified to Service Provider as part of a Data Breach declared by a the Member Company. ID Theft events that are discovered or first known to Affected Consumers prior to the Data Breach event are not eligible for Services under this Agreement.

IF YOU DO NOT AGREE WITH ANY OF THESE TERMS AND CONDITIONS, DO NOT UTILIZE THESE SERVICES.