How Venerable is keeping your accounts safe

Venerable takes numerous measures to safeguard the confidentiality, integrity and availability of our systems, including authentication, monitoring, auditing and encryption. These are built into the design, implementation, and day to day practices of our entire operating environment with the goal of preventing the corruption of data and blocking unknown or unauthorized access to our systems and your accounts.

Our work never stops when it comes to your security and we are constantly evolving our strategies to address and adapt to threats. We believe our proprietary data security programs and our proactive focus on “people, technology and process” give us an advantage in combating constant threats. Here are a few examples of how we put this into action:

Customer verification
No matter how you contact Venerable—by e-mail, online or by phone—we verify your identity before allowing you to access your accounts. When you set up online access to your accounts, you are required to create your own unique username and secret password, allowing you safe and secure access to your accounts. We have proprietary monitoring and other protective procedures in place, such as limits on password entry attempts and multifactor authentication.

Strong encryption
We employ some of the strongest methods of encryption commercially available today, in order to protect personal information such as your username and password or the contents of your portfolio as this data travels from your computer to our systems.

Firewalls
To block unauthorized access, our computer systems are protected by firewalls or electronic barriers designed to prevent unauthorized access to our networks.

Secure e-mail
We encrypt sensitive customer e-mails when sending them outside the Venerable network.

Timed logoff
Our websites automatically log you off after an extended period of inactivity, reducing

the risk that others could access your information from your unattended computer or mobile device.

Security at Venerable worksites
Because we also print and deliver documents containing sensitive personal information, all Venerable work areas are monitored continuously and access is restricted to authorized personnel only. Venerable also enforces a clean desk policy that requires sensitive customer information to be locked away when not in use.

Restricted access to customer data
Just as we limit physical access to our work areas, we also restrict access to systems that store or process customer data, and we continuously monitor access to these systems. Access to our systems is given only to approved and authorized roles within the organization.

Training
Our employees receive thorough training on our security policies and everyone is held accountable for compliance with these policies. Employees who work directly with customers receive additional training on emerging risks, such as phishing e-mails, targeted scams and other forms of identity theft. We also have a dedicated team of cybersecurity professionals who are regularly trained on best practices for combatting advanced cyber threats.

How Venerable Is Keeping You Safe Online

Venerable has implemented numerous security measures to safeguard the confidentiality, integrity and availability of our customer data, including authentication, monitoring, auditing, and encryption. Security measures have been built into the design, implementation and day-to-day practices of our entire operating environment as a part of our continuing commitment to risk management. These measures are designed and intended to prevent corruption of data, block unknown or unauthorized access to our systems and information, and provide reasonable protection of customer information we possess.

Implementing username and password requirements

When you set up online access to your accounts, you create your own unique username and secret password, allowing you safe and secure access to your accounts. We have proprietary monitoring and other protective procedures in place, such as limits on password entry attempts and multifactor authentication.

Customer verification

No matter how you contact Venerable—online or by phone—we verify your identity before allowing you to access your accounts.

Multi-factor Authentication

Venerable will send a Verification Code (also known as a “One-Time Passcode”) via text or email for online activities including, but not limited to, forgotten username or password, online access to your account from a new device. For security purposes, the Venerable Verification Code must be entered at the online prompt to continue.

Strong encryption

We employ some of the strongest methods of encryption commercially available today to protect personal information such as your username and password or the contents of your portfolio as it travels from your computer to our systems.

Firewalls

To block unauthorized access, all of our computer systems are protected by firewalls or electronic barriers designed to prevent unauthorized access to our networks.

Secure email

We encrypt sensitive customer emails when sending the outside the Venerable network.

Timed logoff

Our websites automatically log you off after an extended period of inactivity. This reduces the risk that others could access your information from your unattended computer or mobile device.

Constant systems surveillance

Our security teams monitor our systems around the clock in an effort to secure your information and ensure that only authorized access to your account is permitted.

Security at Venerable worksites

Because we also print and deliver documents containing sensitive personal information, all Venerable work areas are monitored continuously and access is restricted to authorized personnel only. Venerable also enforces a clean desk policy that requires sensitive customer information to be locked away when not in use.

Restricted access to customer data

Just as we limit physical access to our work areas, we also restrict access to systems that store or process customer data, and we continuously monitor access to these systems. Access to our systems is given only to approved and authorized roles within the organization.

Employee education

Our employees receive thorough training on our security policies, and each employee is held accountable for compliance with these policies. Employees who work directly with customers also receive additional training on emerging risks, such as phishing emails, targeted scams, and other forms of identity theft.

More Information

The U.S. Federal Trade Commission provides information on how to avoid phishing scams. Go to onguardonline.gov/phishing.

The Anti-Phishing Working Group (APWG) provides statistics on phishing attacks and advice for individuals and companies. APWG is a global pan-industrial and law enforcement association focused on eliminating fraud and identity theft that result from phishing and other online scams. Go to antiphishing.org.