CYBERSECURITY GLOSSARY

DDOS (DISTRIBUTED DENIAL OF SERVICE) ATTACK

A DDoS attack is a malicious attempt to disrupt or shut down a website by overwhelming the website with a flood of internet traffic.

MALWARE (MALICIOUS SOFTWARE)

A program designed to infiltrate a computer or computer system to steal sensitive information and/or damage a computer or computer system.

PATCH

A software change or update. A patch is often used to repair flaws or bugs in the software as well as introduce new features and capabilities.

PENETRATION TESTING (PENTESTING)

A security test where security experts mimic hackers to expose weaknesses in a computer or computer system.

PHISHING

A message from a hacker that tries to collect sensitive information from you or your business. These messages are dressed up to look like a bank, business or government entity you do business with. Phishing attacks can take place over e-mail, text messages, through social networks or via smartphone apps.

TWO-FACTOR/MULTI-FACTOR AUTHENTICATION

Two or more ways to prove your identity before being allowed access to a site, account or system. This provides an additional layer of security beyond your password.

VULNERABILITY

Any weakness in a computer or software that a hacker could exploit to cause harm.

REGULATORY GLOSSARY

CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

CCPA is legislation designed to protect the privacy rights and collected information of California residents including data held by companies outside of California.

GENERAL DATA PROTECTION REGULATION (GDPR)

GDPR is a European Union (EU) law requiring all businesses, regardless of location, to protect the privacy and personal data collected about EU citizens, including the right of complete data removal.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

HIPAA is a federal law that provides privacy standards to protect patient medical records and other health information provided to health plans, doctors, hospitals and other health care providers.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS (PCI DSS)

Widely accepted set of policies and procedures intended to protect cardholders against misuse of their personal information. The PCI DSS was created jointly in 2004 by four major credit-card companies: Visa, MasterCard, Discover and American Express.

RED FLAGS RULE

A federal regulation that requires financial institutions to have an official plan and process in place designed to protect consumers from identity theft.

* All of the above are general terms which may vary based on context. Please consult the quote or ask an agent/broker for precise definitions and details.