1. What is Multi-factor authentication?

Multi-factor authentication (**MFA**; **two-factor authentication**, or **2FA**, along with similar terms) is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism. MFA protects personal data which may include personal identification or financial assets from being accessed by an unauthorized third party that may have been able to discover any account details which help them to gain access to your online data.

When you sign into your online accounts, with additional authentication, you are proving to the service that you are who you say you are. Traditionally that's been done with a username and a password. Unfortunately, this is not the securiest or safest way to do it. Usernames are often easy to discover; sometimes they're just your email address and since passwords can be hard to remember, people tend to pick simple ones, or use the same password on various different websites.

That's why almost all online services - banks, social media, shopping and yes, Marsh too - have added a way for your accounts to be more secure. You may hear it called "Two-Step Verification" or "Multi-factor Authentication" but they all operate off the same principle. When you sign into the account for the first time on a new device or app, like a web browser, you will need more than just the username and password. You will need a second verification method or “Second Factor” to prove who you are.

2. Why is Multi-factor authentication necessary?

Digital security is critical in today's world because both businesses and users store sensitive information online. Everyone interacts with applications, services, and data that are stored on the internet using online accounts. A breach, or misuse, of this online information could have serious real-world consequences, such as financial theft, business disruption, and loss of privacy.

While passwords protect digital assets, they are simply not enough. Expert cybercriminals try to actively find passwords. By discovering one password, access can potentially be gained to multiple accounts for which you might have reused the password. Multi-factor authentication acts as an additional layer of security to prevent unauthorized users from accessing these accounts, even when the password has been stolen. Businesses use multi-factor authentication to validate user identities and provide quick and convenient access to authorized users.

3. What are the benefits of Multi-factor authentication?

Reduces security risk

Multi-factor authentication minimizes risks due to human error, misplaced passwords, and lost devices.

Enables digital initiatives

Organizations can undertake digital initiatives with confidence. Businesses use multi-factor authentication to help protect organizational and user data so that they can carry out online interactions and transactions securely.

Improves security response

Companies can configure a multi-factor authentication system to actively send an alert whenever it detects suspicious login attempts. This helps both companies and individuals to respond faster to cyberattacks, which minimizes any potential damage.

4. How does Multi-factor authentication work?

Multi-factor authentication works by requesting multiple forms of ID from the user at the time of account registration. The system stores this ID and user information to verify the user for next login. The login is a multi-step process that verifies the other ID information along with the password.

Let's say you're going to sign into your Marsh account, and you enter your username and password. If that's all you need then anybody who knows your username and password can sign in as you from anywhere in the world!
But if you have multi-factor authentication enabled, things get more interesting. The first time you sign in on a device or app you enter your username and password as usual, then you get prompted to enter your second factor to verify your identity.

Some people worry that multi-factor authentication is going to be really inconvenient, but you won't have to do the second step if you're logging in from the same device within 24 hours. All you need to do is select *"remember my device*" on the multi-factor authentication page when you first log into your account. After that you'll just need your primary factor, usually a password, like you do now.

The extra security comes from the fact that somebody trying to break into your account is probably not using your device, so they'll need to have that second factor to get in. Compromised passwords are one of the most common ways that criminals can get at your data, your identity, or your money. Using multi-factor authentication is one of the easiest ways to make it a lot harder for them.

If somebody else tries to sign in as you, they'll enter your username and password, and when they get prompted for that second factor they're stuck! Unless they have your smartphone, they have no way of getting that 6-digit number to enter. We describe the steps in the multi-factor authentication process below:

Multi-factor Registration

- A user creates the account with username and password. They then link other items, such as a mobile phone device or computer device to their account. The item might also be virtual, such as an email address, a mobile phone number, or authenticator app code. All these items help to uniquely identify the user and should not be shared with others.

Authentication

- When a user with MFA-enabled logs into a website, they are prompted for their username and password (the first factor–what they know), and an authentication response from their MFA device (the second factor–what they have).
- If the system verifies the password, it connects to the other items. For example, it may issue a number code to the hardware device or send a code by SMS to the user's mobile device.

System Access

- The user completes the authentication process by verifying the other items. For example, they might enter the code they have received or press a button on the hardware device. The user gets access to the system only when all the other information is verified.

5. Need assistance?

Should you have any questions or concerns about multi-factor authentication or require any other further information about your account and insurances, please contact your usual insurance representive as noted on your policy documentation.