Multi-Factor Authentication FAQs

1. **What is Multi-factor Authentication (MFA)?**
   Multi-factor authentication (MFA) is a security system that requires more than one piece of evidence (known as a ‘factor’) to authenticate the user for login or other transaction.

   Entering your username and one password alone is considered a single-factor authentication. Multi-factor Authentication (MFA) adds a second level of authentication to an account log-in, decreasing the likelihood that others can compromise your account.

   With PT-X MFA the factors (evidence of identity) are:
   
   - Something you know, your user name & password
   - Something you have, a one-time pass code (OTP) from the PT-X MFA token or PT-X authenticator app

2. **Why do I need to use Multi Factor Authentication?**
   Passwords alone can be challenging to secure, they can be written down by users, stolen, guessed and new technology and hacking techniques like rainbow tables for common password combinations means online can be increasingly targeted. MFA adds a second layer of security to your account to make sure that your account stays safe, even if someone else guesses or knows your password.

   Multi factor authentication of users helps to ensure only authorised personnel are accessing the system, and is becoming commonplace – your Bank, e-Mail provider & even social media provider use MFA today to secure their clients.

3. **What options do we have to secure our users authentication details in line with MFA changes in PT-X?**
   Multi Factor Authentication is now a standard function of PT-X, available to every user without charge. It is no longer an optional module, and we will require all users to enable it on their accounts, PT-X will also no longer support login without a second factor. We consider this to be the minimum level of security to ensure our user community remains protected against threats.

   All PT-X users have the choice to use a simple and straightforward key-fob style one time passcode token, or a PT-X OTP Authenticator app (available on both iOS and Android versions) to access PT-X.

4. **How does Multi Factor Authentication work?**
   When you log in to PT-X, as well as your user name & password you must additionally enter the one-time passcode generated by the Key-fob token or PT-X authenticator app.

   The key-fob tokens are ideal for authentication applications where portability and ease of use are paramount. These small devices fit comfortably on a key ring in any pocket or purse. A simple push of a button generates a one-time passcode. These tamper-resistant devices can be used wherever strong authentication is required.

   If using the PT-X Authenticator App, downloaded once registered with PT-X by scanning an on-screen QR code, each time you go into the app or refresh a one-time passcode is generated. The app can be downloaded from the Apple app store, or Google Play store for Android devices without charge.
5. **What if our corporate IT policy does not allow Mobile Apps to be deployed on my phone?**

   Should you choose not to or, not be able to use the Bottomline Mobile App(s), we offer the alternative option of a simple and straightforward ‘key-fob’ token to access PT-X.

6. **What if I don't want to install an app on my phone?**

   We offer a simple and straightforward ‘key-fob’ token to access PT-X through our account team.

7. **Will I need to change my password?**

   No. MFA is an additional layer of security entirely independent of your existing login credentials.

8. **Does MFA see my password?**

   PT-X verifies your Internet password with its internal systems as before, and never sends it to MFA. MFA provides only the second factor—the “something you have.” In fact, MFA tokens or App have no direct communication with PT-X—just enough information is used (a ‘seed value’ so it can do its job).

9. **Do we need to have tokens for admin users or just entry/release users?**

   To ensure the safety of our user community, and the many companies that rely on PT-X for their business, we require that all PT-X users are protected by MFA and we will not support log-in without a second factor (token or PT-X Authenticator app).

10. **Can we source the ‘key fob’ tokens ourselves?**

    Each key fob token is configured specifically by Bottomline; we supply and manage by the security and registration process. 3rd Party tokens cannot be used.

11. **What happens should I decide to “take the risk” and just rely on User ID & password?**

    To keep up with the fast paced industry changes and cyber fraud threats, all PT-X users must use a second factor upon their login.

12. **Can we have a token shared between users?**

    No, tokens are issued to companies and registered by an individual – which directly associates to their login ID within the PT-X service. This authentication factor that is presented cannot be used by another user to support individual accountability of access to services and applications.

13. **We already have MFA enabled. Is there further protection available around our payments?**

    Whilst MFA is to become standard practice for PT-X, this is minimum security requirements. We strongly recommend that you protect your payments with the PT-X Security Pack to minimise your risk to fraud.

14. **Will MFA be prevalent when the changes associated with Open Banking and PSD2 are introduced?**

    What we’re used to seeing as consumers and in the banking world is coming the way of the corporate; ‘Strong Customer Authentication’ will be a requirement within Open Banking & PSD2. To raise adoption dramatically, a change in our approach to the market is needed that builds on the concept of protecting our clients & their critical payments. This change will be that we will raise the security level of PT-X for our client community by ensuring that all clients must have MFA enabled.

*For more information please contact your account manager by email or call +44 (0) 118 925 8250.*