Bottomline Technologies

DATA SHEET

Multi-Factor Authentication FAQs

1. **What options do we have to secure our users authentication details in line with the SWIFT mandate?**
   Soft and hard tokens are both options to secure user authentication details.

2. **What is the difference between soft and hard tokens?**
   GTExchange Multi-Factor Authentication (MFA) via soft tokens involves secondary validation through a mobile device (smartphone or tablet) also available as Winauth application straight to your desktop. Hard (RSA) tokens are physically accessed as a managed service from the Bottomline Bureau.

3. **When will soft and hard tokens be available from Bottomline?**
   Soft token access is available today, hard tokens will be available to users by May 2017 at the latest.

4. **What is the option if our corporate policy does not allow iPhones for soft token access?**
   Soft token access is also enabled for android phones or to your desktop through a Windows desktop application as an alternative (our account managers will go through this option in detail). Or companies can wait for hard token availability.

5. **Can we have access to soft tokens ahead of hard tokens being available?**
   Yes – this is possible and would be managed in such a way to not disadvantage companies commercially.

6. **Can we phase in the use of user tokens or do we have to adopt a big bang approach to implement tokens?**
   It is possible to phase in use of user tokens over time rather than have a big bang approach.

7. **Do we need to have tokens for admin users or just entry/release users?**
   Remember that part of the “standard” modus operandi is the masking of fraudulent activity, this is carried out by the attackers with knowledge that has been in gained in reviewing and monitoring the operations. SWIFT mandates that all users are protected.

8. **Can we source the soft / hard tokens ourselves?**
No – we supply tokens which is supported and managed by Bottomline.

9. **What happens should I decide to "take the risk" and just rely on User ID & password.**
As part of the SWIFT Customer Security Programme (CSP), the MFA is now mandatory and non-compliance with this control will flag up on future SWIFT audits as a breach and published to the SWIFT community.

10. **Can we have a token shared between users?**
No, tokens are issued to individuals and directly linked to their login ID within the Bottomline infrastructure. SWIFT states: "The authentication factors that are presented must be personal and support individual accountability of access to services and applications."

11. **Do the cyber fraud attacks affect just SWIFT FIN or FileAct as well?**
The cyber fraud attacks appear to have focused on SWIFT FIN, however FileAct can also be compromised following the same attack vectors into a customer's infrastructure. Bottomline considers all of its services are in scope.

12. **Does cyber fraud affect Fast Payment Service (FPS) and Bacs?**
The recently published SWIFT breaches do not include FPS and Bacs, but the same attack modus operandi could be used to attack a user's operation of these services.

13. **Can the tokens provide additional coverage for Bacs and FPS security?**
Yes, for user access, the tokens can be utilised to secure access into the Bottomline infrastructure for these services

14. **Can Bottomline help with the mandatory controls for detecting anomalous activity? Our IT teams have said this would be difficult.**
Yes, our Payment Fraud for SWIFT solution uses state of the art technology to detect anomalous transactions and user behavior and present real-time notifications and stop payments. This is a simple add-on service for our GTExchange Bureau customers.

15. **We have MFA already, when can I have the transaction monitoring solution?**
This is available to order now, with implementation currently scheduling for May.

16. **When do I need to have updated controls implemented?**
SWIFT states end of June you must be in a position to self-attest. We strongly recommend planning now, and implementing changes by June to fit in line with the deadlines.

17. **We meet the vast majority of CSP controls already, and some are seen as absolute minimum, what is Bottomline's view of this?**
For some SWIFT users this will be a big leap in meeting the standards. Overall, we welcome the raising of the bar for all SWIFT users.

Our solutions help with relevant controls and aim to over and achieve the standards. This is ultimately about reducing risk of fraud and error, and our services and technology additions shared today aim to focus on that solid good practice.

For more information please contact your Account Manager by *email* or call +44 (0) 207 105 0100.

CONTACT

Connect with us

EMEA Headquarters
115 Chatham Street
Reading, England
Berks RG1 7JXI United
Phone (Local): 0118 925 8250
Phone (Int) : +44 118 925 8260
emea-info@bottomline.com

London Office
10 Aldersgate Street
London, England
EC1A 4HJ
Phone (Local): 0207 105 0100
Phone (Int) : +44 (0) 207 105 0100
emea-info@bottomline.com

bottomline.com