**SSL安全策略升级通知**

尊敬的商户，您好：

HTTPS加密协议SSLv3、TLS1.0都已经曝出过高危漏洞，可能导致网络中传输的加密数据被黑客监听破解，对用户信息、网络账号密码、交易信息等安全构成威胁。为保证通信安全，我司服务器将于19年6月30日关闭掉SSLv3、TLS1.0版本支持，不再支持使用SSLv3、 TLS1.0或更低版本的客户端调用。请仍在使用这些版本的商户于19年6月30日前务必修复升级完成。  
        示例1（java）  
        SSLConnectionSocketFactory sslsf = new SSLConnectionSocketFactory(  
                 sslcontext, new String[] { "TLSv1.1" }, // TLSv1.1 TLSv1.2;  
                 null, SSLConnectionSocketFactory.BROWSER\_COMPATIBLE\_HOSTNAME\_VERIFIER);  
          
示例2（php）  
        curl\_setopt($curl, CURLOPT\_SSLVERSION, CURL\_SSLVERSION\_TLSv1\_1); // CURL\_SSLVERSION\_TLSv1\_1 CURL\_SSLVERSION\_TLSv1\_2  
          
示例3（C#）  
        System.Net.ServicePointManager.SecurityProtocol = SecurityProtocolType.Tls11 // SecurityProtocolType.Tls11  SecurityProtocolType.Tls12  
  
        我司提供的测试域名：**[https://tls-pay.ipaynow.cn](https://tls-pay.ipaynow.cn/" \t "https://exmail.qq.com/cgi-bin/_blank)** （生产环境域名保持不变，仍为 pay.ipaynow.cn）  
        在该环境下，如果通过低版本的SSL调用接口，将会直接报错，提示连接失败。请各位商户务必认真测试并及时反馈，感谢您的配合！  
  
**需要贵司技术做两件事：  
        1.确认下自己的SSL 版本是否符合标准  
        2.测试下我们提供的测试接口是否有异常。**  
  
感谢一直以来对我司的支持和配合，我们致力为贵司提供更好地服务，敬请期待！如有其他疑问，请随时联系我们。  
       电话：4006-365-303