La Directiva sobre servicios de pago revisada

Por Steven D'Alfonso y Assaf Regev

Introducción

Durante las últimas tres décadas, hemos sido testigos de grandes cambios tecnológicos en el mundo de los servicios financieros... y de las dificultades que encuentran los reguladores para seguir su ritmo. Por ejemplo, los proveedores de servicios de pago electrónico, como PayPal (posteriormente adquirido por eBay) asumieron el reto de facilitar los pagos online en todo el mundo. La propuesta de PayPal era simple: un servicio de pagos online fácil de usar que actuara como alternativa a los métodos de pago en papel tradicionales, como cheques y giros postales, u otros costosos métodos de transferencia electrónica. Esto supuso una revolución para usuarios y vendedores online, pero causó muchos quebraderos de cabeza a los reguladores.

A finales de 2007, el Parlamento Europeo y el Consejo de la Unión Europea promulgaron la Directiva sobre servicios de pago (PSD, según sus siglas en inglés). La PSD debe su creación a varios motivos[1]:

Fomentar un mercado de pagos más integrado y eficiente
Ayudar a equilibrar el campo de juego entre los proveedores de servicios de pago (incluyendo a los nuevos participantes)
Lograr que los pagos sean más seguros
Proteger a los consumidores
Promover la aplicación de comisiones más bajas sobre los pagos

En 2011 se constituyó la Autoridad Bancaria Europea (ABE) con el fin de garantizar la homogeneidad de la normativa en todo el sector bancario europeo. El principal cometido de la ABE es "*contribuir a la creación de un código normativo único europeo para la banca que tiene por objeto proporcionar un mismo conjunto de normas prudenciales armonizadas para las instituciones financieras de toda la UE*".[2]

En diciembre de 2015, el Parlamento Europeo promulgó una Directiva sobre servicios de pago revisada (PSD2) que reemplaza y amplía la directiva original de 2007. El rápido crecimiento y las innovaciones tecnológicas en el ámbito de los pagos online y móviles hizo necesaria esta directiva revisada. Los objetivos de la PSD2 son claros y acordes con la normativa que actualiza: en lugar de limitar su competencia a la rígida supervisión de las transacciones, su finalidad es aumentar la transparencia, facilitar nuevas metodologías para servicios de pago y ayudar a reducir los costes a través de la competencia facilitando la entrada en el mercado de servicios de pago.

PSD2: Una nueva gran oportunidad

PSD2 presenta oportunidades e introduce nuevos requisitos para los bancos. Las organizaciones proactivas que la adopten de inmediato podrán responder a las nuevas demandas con rapidez. Con la creación de nuevas alianzas y ofreciendo servicios innovadores, podrán generar valor tanto para sí mismas como para sus clientes.

Al abordar los nuevos requisitos de seguridad que puedan derivarse de PSD2, bancos e instituciones financieras deberán contemplar la actualización de sus estrategias de negocio y seguridad para sostener los ingresos y retener a sus clientes.

Cabe señalar que los bancos y otras instituciones financieras europeas disponen de un plazo limitado para prepararse con vistas a estos cambios, ya que PSD2 será aplicada por los reguladores gubernamentales a principios de 2018.

¿Cuáles serán sus efectos para los proveedores de servicios de iniciación de pagos?

Un proveedor de servicios de iniciación de pagos (PISP, según sus siglas en inglés) es un tercero que facilita el pago online entre usuarios finales y comercios online. El PISP proporciona una plataforma que ayuda a confirmar que los fondos necesarios existen en la cuenta bancaria del usuario (ver Figura 1). El usuario debe autorizar al PISP ante el banco o un proveedor de servicios de pago tradicionales mediante cuentas (ASPSP, según sus siglas en inglés) antes de iniciar el primer pago. El PISP actúa entonces como un embudo a través del cual los usuarios acceden a sus cuentas bancarias y emiten órdenes de pago. Ahora todos los requisitos de comunicación y autenticación recaen en los PISPs cuando contactan con un ASPSP.

Cronograma previsto para la implantación de la Directiva de servicios de pago revisada (PSD2)

2015

JUNIO
Publicación de las normas de PSD2

JULIO
Entrada en vigor de PSD2

AGOSTO
Entrada en vigor de las normas de la Autoridad Bancaria Europea (ABE) sobre la seguridad de los pagos en Internet

2016

JULIO
Presentacion del proyecto de normas técnicas reguladoras de la ABE (NTR)

SEPTIEMBRE
La Comisión Europea refrenda las NTRs

OCTUBRE
EBA enmienda el proyecto de las NTRs

DÍA D (FINALES DE 2016)
Entrada en vigor de las NTRs

2017

JULIO
Los Estados Miembros promulgan y publican leyes, reglamentos y disposiciones administrativas para el cumplimiento de PSD2

2018

DÍA D + 18 MESES (PRINCIPIOS DE 2018)
Los Estados Miembros velan por la aplicación de las NTRs

Figura 1. Secuencia de hitos clave durante la implantación de la Directiva de servicios de pago revisada (PSD2) de la Unión Europea

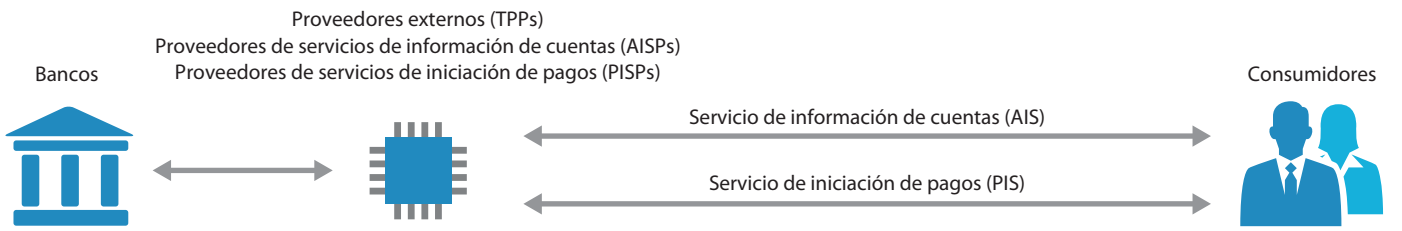

Figura 2. PSD2 permite a los proveedores externos (TPPs) acceder a sistemas de procesamiento de pagos bancarios e información de cuentas.

Según una reciente actualización normativa de Accenture Consulting,[3] los nuevos requisitos afectarán probablemente a casi todos los aspectos del negocio de los proveedores de servicios de pagos (PSP): productos, servicios, operaciones, colaboraciones y unidades de atención al cliente. Es posible que los PSPs deban reorganizar todo su modelo y estrategia de negocio, incluyendo sus departamentos de negocio, riesgo, conformidad y TI, para adaptarse de modo efectivo y puntual a los cambios requeridos. A continuación se exponen someramente algunos de los retos potenciales que afrontan los participantes de este mercado:

Incremento potencial del **riesgo de seguridad** con la introducción de un tercero entre la institución financiera y el consumidor
Preocupación por la protección de datos suscitada por el hecho de que la protección de datos personales es especialmente prioritaria para los reguladores europeos y merece atención especial; ver aquí un ejemplo reciente de intervención normativa europea en el mundo de los medios sociales
Reclamaciones de responsabilidad en caso de transacciones no autorizadas y fugas de datos

¿Cuáles serán sus efectos para los usuarios?

Los principales beneficiados por este cambio normativo son los usuarios finales del banco (los consumidores), en gran parte porque podrán consolidar todas sus cuentas de pago. Esto ofrece la oportunidad de elegir la interfaz web o aplicación más conveniente para comprobar sus detalles online. Se beneficiarán, además de la integración directa de sus cuentas bancarias en sitios de comercio online (como Amazon) para disfrutar de una experiencia cómoda y fluida en sus compras.

Los cambios normativos también pueden resultar en un reforzamiento de las medidas de seguridad ("autenticación de clientes avanzada") con el fin de mejorar la experiencia de los usuarios sin complicaciones asociadas a la seguridad. Esta mejora del proceso de autenticación de usuarios requiere el uso de dos o más elementos independientes, clasificados como:

Conocimiento: Algo que solo el usuario *conoce*, como una contraseña o un dato personal
Posesión: Algo que solo el usuario *posee*, como un identificador o un aparato (smartphone) que el usuario debe demostrar que obra en su poder en el momento de iniciar sesión (normalmente mediante una contraseña de un solo uso)
Inherencia: Algo que el usuario *es*; puede tratarse de características físicas únicas, como las huellas dactilares o el iris, o bien biométricas de comportamiento, como pautas de navegación u otros rasgos

Estos elementos deben ser independientes, de manera que la potencial violación de uno no comprometa la fiabilidad de los demás. También deben estar diseñados para proteger la confidencialidad de los datos de autenticación.

Un aspecto negativo es que, en caso de fraude o pérdida económica, los consumidores que busquen una compensación pueden encontrar confusa la relación y las responsabilidades existentes entre PISPs, vendedores y bancos u otros ASPSPs.

Retos de las organizaciones financieras

En lo que se refiere a las organizaciones comerciales, especialmente los bancos y otras instituciones financieras, se avistan otros retos en el horizonte.

Con arreglo a PSD2, los bancos y otras instituciones financieras buscarán adaptar sus modelos de negocio y forjar nuevas relaciones para crear servicios innovadores que contribuyan a compensar las inversiones iniciales y permanentes. Por otra parte, si bien la normativa no exige interfaces de programación de aplicaciones (APIs) para facilitar estos nuevos modelos, la comunicación basada en APIs es, posiblemente, la vía más lógica que elegirán los bancos. Por este motivo, tanto los bancos como otras instituciones financieras deberían contemplar el desarrollo de nuevos estándares técnicos para facilitar la interoperabilidad.

PSD2 y defraudadores

Los ciberdelincuentes son expertos en la explotación de tecnologías y procesos creados en beneficio de instituciones financieras y usuarios. La introducción de nuevos mecanismos de pago en virtud de PSD2 puede ofrecer a los delincuentes formas de infiltrarse en los sistemas de pago. Las amenazas externas podrían apuntar directamente a las APIs de bancos, PISPs y ASPSPs; los defraudadores son hábiles detectando vulnerabilidades.

Aunque los PSPs son miembros relativamente recientes de los servicios financieros, los bancos luchan contra el fraude desde hace mucho tiempo y han invertido grandes sumas en la prevención y detección del fraude. Sin embargo, y pese a todos sus esfuerzos, el número de fraudes cometidos contra los bancos y sus clientes no ha disminuido. Aunque la tecnología ha ayudado a mitigar ciertos puntos débiles, el resultado general es que el fraude simplemente se desplaza a otros dominios menos protegidos.

Combatir el fraude se asemeja en gran medida al famoso juego de los topos o "Whack-A-Mole": cuando se golpea al topo, aparece otro en su lugar. Pero con la aparición de nuevos participantes a causa de PSD2, es posible que aparezcan varios "topos" defraudadores por cada uno golpeado. Los proveedores externos, tanto nuevos como ya existentes, quizá carezcan de la misma sofisticación en su infraestructura de seguridad que poseen los bancos. Los expertos del sector predicen que la autenticación multifactor que conocemos experimentará una importante evolución en el momento en que la PSD2 sea de aplicación, en 2018-2019.[4]

Desde que los proveedores de servicios de pago electrónico hicieran acto de aparición hace más de 15 años, los defraudadores han hecho del eslabón más débil, normalmente los seres humanos, y especialmente los consumidores, su objetivo. Aunque el riesgo de fuga de datos persiste, el modo más fácil de infiltrarse en el proceso de pago consiste en comprometer los dispositivos de los consumidores o engañar a los mismos consumidores.

Un método de ataque frecuente combina ingeniería social y malware en el dispositivo del consumidor. En este caso, los ciberdelincuentes diseñan cuidadosamente un malware destinado a efectuar una inyección web en un distribuidor online para comprometer el proceso de pago. La inyección suele producirse en la etapa de pago, abriendo una página falsa que solicita al usuario información de seguridad adicional para "confirmar" los ajustes de seguridad o realizar otra tarea. Si el cliente obedece, el defraudador obtiene información de seguridad fundamental relacionada con el PISP.

¿Cuánta gente cae en la trampa de esta clase de ataque y entrega información confidencial a los delincuentes? La respuesta es que mucha. La página falsa aparece al final de la sesión online del cliente, cuando este quizá se sienta seguro porque la experiencia de compra ha sido normal hasta ese momento.

Podemos especular acerca de cómo los ciberdelincuentes y defraudadores se aprovecharán del proceso, tal y como se hace a continuación, pero es probable que exista al menos un modo que nadie ha contemplado aún. La ley de las consecuencias imprevistas está casi siempre presente cuando se trata de nuevas tecnologías u ofertas de servicios financieros.

A continuación se expone una breve lista de tácticas empleadas por ciberdelincuentes y defraudadores para explotar el proceso de pago. No es una lista exhaustiva, pero destaca algunos de los métodos más comunes:

Fuga de datos: El riesgo de un ciberataque directo contra un banco o proveedor externo es constante. Los bancos desarrollan respuestas a estas amenazas directas sin descanso. PISPs y ASPSPs, por el contrario, quizá no dispongan de una infraestructura tan consolidada, lo que podría incrementar el riesgo. Algunas fugas notorias en compañías financieras han sido el resultado de ataques "Spear-phishing". Los bancos han formado a su personal para detectar mensajes de correo electrónico de phishing y otras tácticas de ingeniería social similares. Por este motivo, los ciberdelincuentes dirigen su atención hacia los nuevos proveedores externos.

Filtración en API: El desarrollo de la banca y los pagos a través de API ofrece a los defraudadores un nuevo dominio que explorar. Una autenticación o protección insuficiente del acceso API puede proporcionar un acceso directo a los sistemas del proveedor de servicios a través del cual podrían inyectarse instrucciones de pago masivas.

Usuario comprometido: Tanto si los proveedores de servicios de información de cuentas (AISPs, según sus siglas en inglés) ofrecen nuevos servicios y experiencias bancarios como si los PISPs simplifican los medios de pago de sus aplicaciones de comercio electrónico o móvil, el acceso de los usuarios a los servicios puede resultar comprometido debido al empleo de diversos métodos para la extracción de credenciales, como:

- *Phishing:* Estos ataques persuaden a los usuarios para que revelen sus credenciales de acceso privadas. Aunque el uso de la autenticación multifactor se ha generalizado, los delincuentes más hábiles han demostrado ser capaces de superar dicha autenticación y el uso de contraseñas de un solo uso mediante información obtenida por medio de phishing.
- *Malware:* Es posible diseñar malware capaz de infiltrarse en PISPs y ASPSPs, del mismo modo que en los bancos, para robar datos de clientes de sus sistemas. Sin embargo, es más probable que el malware ataque a los usuarios finales. En este caso, el código del malware selecciona como blanco a múltiples organizaciones y se envía a los dispositivos móviles de los consumidores. El malware permanece inactivo, a la espera de que el usuario acceda a un sitio web o aplicación que se cuente entre sus blancos. El método de ataque incluye el robo de credenciales mediante "Man-in-the-Browser" y ataques de superposición, el robo de identificadores de autenticación multifactor e incluso el secuestro completo del acceso remoto para efectuar transacciones desde el mismo dispositivo del usuario en "tiendas" falsas.
- *Ingeniería social:* No siempre se trata de una táctica de fraude en sí. La moderna ingeniería social combina de forma muy sofisticada dos o más elementos que entrañan tecnología, canales de comunicación y el simple engaño. Las campañas de phishing pueden ser simples mensajes de correo electrónico con un documento adjunto malicioso o complejos métodos que incitan a los clientes a llamar al "servicio de atención" para solucionar un problema urgente, momento en el que el defraudador intenta convencer al cliente para que revele información confidencial o actúe de algún modo. Cada paso del proceso tiene como fin inspirar confianza al cliente para que revele los datos que el defraudador necesita para actuar contra la cuenta
del consumidor.

Soluciones de protección contra el fraude IBM Security Trusteer

Las soluciones IBM® Security Trusteer® ayudan a las organizaciones a satisfacer sus necesidades de seguridad con capacidades que incluyen, entre muchas otras, la validación de autorizaciones de clientes e identidades online.

IBM Security Trusteer Pinpoint™ Detect ofrece recomendaciones en tiempo casi real sobre intentos de inicio de sesión, caducidad de sesiones y validez de las autenticaciones. Gracias a estas capacidades, las organizaciones pueden validar a los usuarios online en todos sus dispositivos de manera precisa y sin frustración alguna para estos. Este eficaz análisis pasivo hace que el proceso de seguridad sea mucho más difícil de burlar para los defraudadores, ya que para ellos es mucho más complejo combatir lo que no pueden ver.

Mediante la agregación y correlación de inteligencia de amenazas basada en la evidencia, indicadores de riesgo, analíticas de comportamiento e información de fraudes detallada, Trusteer proporciona recomendaciones prácticas para la detección de fraudes e identidades con las que las organizaciones pueden hallar un equilibrio entre la seguridad y la comodidad del usuario al tiempo que se concentran en su actividad principal.

IBM Security Trusteer Pinpoint Detect ayuda creando dos capas de evaluación independientes para la validación de identidades en una misma solución. Trusteer Pinpoint puede alertar al PSP cuando un dispositivo compatible perteneciente a un usuario comprometido, o en manos de un defraudador, intenta acceder a una aplicación protegida (incluyendo aplicaciones web y móviles). Con el fin de detectar el acceso fraudulento a las cuentas, la solución recoge información para generar una "huella dactilar" del dispositivo y etiqueta los dispositivos de los defraudadores. También observa, de forma independiente, el comportamiento de los usuarios, detecta la suplantación de dispositivos o la ocultación en proxies e identifica herramientas de acceso remoto, lo que le permite comparar la sesión y el comportamiento del usuario con interacciones anteriores y crear un perfil de comportamiento consistente que pueda utilizarse para facilitar el acceso de los usuarios a los servicios.
IBM Security Trusteer Mobile SDK proporciona un identificador de dispositivo unívoco (ID de dispositivo) que ayuda a los proveedores de sistema a distinguir más eficazmente diferentes dispositivos pertenecientes al mismo usuario. Esto incluye nuevos dispositivos detectados y dispositivos asociados a varias cuentas. Además, Trusteer Mobile SDK facilita la identificación de multitud de riesgos que podrían comprometer los dispositivos empleando Trusteer Pinpoint Detect junto con información histórica sobre los accesos del usuario en todos sus dispositivos.
IBM Security Trusteer Rapport®, una vez instalado en el dispositivo del usuario final, ayuda a protegerlo contra ataques avanzados mediante malware y phishing destinados a sustraer información del usuario. Instalado en el dispositivo en cuestión, Trusteer Rapport genera una ID de dispositivo persistente que es resistente a que pueda ser comprometido o reutilizado. Dicha ID, además, será utilizada por Trusteer Pinpoint Detect para reforzar aún más la asociación entre dispositivo y usuario.

Seguridad o comodidad... ¿Por qué no ambas?

Las soluciones IBM Security, y muy especialmente Trusteer Pinpoint Detect, pueden ayudar a los bancos y otras instituciones financieras a controlar el acceso de los nuevos participantes a sus sistemas desplegando sólidas medidas de seguridad que contribuyan a proteger tanto al destinatario del pago como la infraestructura del servicio de pago.

Conclusión

Los piratas informáticos suelen estudiar el comportamiento del usuario final y de las cuentas antes de pasar al ataque. Son expertos en superar medidas de seguridad, como los controles basados en riesgos y los mecanismos de autenticación más eficaces. Por este motivo, los controles de seguridad estáticos son ineficaces a la hora de detener el fraude financiero online.

Los desarrolladores de Trusteer emplean los siguientes métodos fundamentales para ayudar a proteger a los clientes:

Evaluación de riesgos en tiempo real basada en inteligencia. La detección temprana de cambios en el panorama de amenazas es esencial para mantener un proceso de evaluación de riesgos eficaz y levantar defensas capaces de proteger a los clientes frente al fraude online. El equipo de investigación y desarrollo de IBM X-Force® adapta constantemente su índice de inteligencia de amenazas y actualiza las capas de seguridad para ayudar a mitigar riesgos en tiempo real.
Seguridad por capas para la banca y los pagos online. Empleando múltiples capas de seguridad en el terminal y las aplicaciones web es posible establecer una protección potente y flexible. La seguridad en el terminal proporciona una capa de capacidades de defensa, inteligencia y reparación. La detección de malware sin cliente constituye la siguiente capa, cubriendo los sistemas de los usuarios con una implantación de impacto reducido. La combinación de Trusteer Rapport o Trusteer Mobile SDK (para la protección de terminales) con Trusteer Pinpoint (para la detección sin cliente) permite a las organizaciones ayudar a proteger tanto al destinatario del pago como la infraestructura de los servicios de pago. Ambas soluciones pueden emplear la identificación "dactilar" de dispositivos para verificar que un dispositivo concreto obra en poder del usuario final.

Protección de dispositivos de clientes. En años recientes, los ciberdelincuentes han empleando malware capaz de eludir numerosos controles de seguridad. Evitar que este malware infecte el terminal y ataque el navegador o la aplicación web puede ayudar a evitar el fraude. Trusteer Rapport ofrece varias capas de protección para blindar el dispositivo del usuario contra infecciones de malware y ataques de phishing al tiempo que protege las sesiones del navegador web para evitar la manipulación de las transacciones del cliente.

Detección de anomalías. La detección y la prevención temprana de ataques de malware contribuye a reducir el número de transacciones sospechosas que debe atender el personal de prevención de fraudes y soporte, así como los costes de explotación y las necesidades de dotación de personal resultantes. Trusteer emplea sus capacidades de aprendizaje artificial para construir de manera transparente minuciosas descripciones de comportamiento personalizadas basadas en sesiones anteriores con el fin de permitir la comparación entre el comportamiento actual e interacciones precedentes como medio para detectar anomalías que podrían ser síntoma de una infección de malware.

Minimizar el impacto sobre los usuarios finales. El equilibro entre seguridad, facilidad de uso e interoperabilidad promueve la adopción por parte del usuario y minimiza el impacto sobre el flujo de trabajo diario sin comprometer la seguridad.

Colaboración con una empresa de prevención del fraude bancario de eficacia demostrada. En última instancia, combatir el fraude es un trabajo en equipo. Las instituciones de servicios financieros deben seleccionar proveedores en función de su capacidad para aportar a su personal conocimientos y capacidades que permitan levantar una defensa eficaz contra los ciberdelincuentes.

Información adicional

Para obtener más información sobre las soluciones IBM Security Trusteer, póngase en contacto con su representante IBM o IBM Business Partner, o visite: **ibm.com**/software/products/en/category/advanced-fraud-protection

Glosario

AISP (proveedor de servicios de información de cuentas): Una de las dos nuevas categorías de proveedores de pagos externos (TPP, según sus siglas en inglés) introducidas por PSD2. Un AISP actúa como agregador de datos en relación con las cuentas que un usuario posee en uno o varios ASPSPs diferentes. Los AISPs deben registrarse como institución de pagos conforme a PSD2.

ASPSP (proveedor de servicios de pago mediante cuentas**):** Tipo de institución de pago tradicional en la que un usuario posee una o más cuentas.

PISP (proveedor de servicios de iniciación de pagos): Segunda nueva categoría de TPP introducida por PSD2. El usuario autoriza a los PISPs a iniciar pagos en su nombre. Funcionan estableciendo un "puente" de software entre el sitio web del comerciante y la plataforma bancaria online del banco del pagador con el fin de iniciar el pago. Normalmente el PISP está disponible como opción de pago en el sitio web comercial.

PSP (proveedor de servicios de pago): Denominación general para aquellos proveedores que ofrecen servicios online para la aceptación de pagos electrónicos mediante diversos métodos, como tarjetas de crédito o débito y transferencias en tiempo real. A los PSPs tradicionales, como bancos e instituciones financieras, se une ahora un conjunto cada vez más amplio y heterogéneo de TPPs.

IBM Security
Route 100
Somers, NY 10589

Producido en los Estados Unidos de América
Noviembre 2016

[1] "LIBRO VERDE Hacia un mercado europeo integrado de pagos mediante tarjeta, pagos por Internet o pagos móviles", *EUR-Lex*, Documento 52011DC0941, 11 de enero de 2012. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1476195234402&uri=CELEX:52011DC0941

[2] "About Us", *Autoridad Bancaria Europea*. http://www.eba.europa.eu/about-us

[3] "Welcoming a new phase of Everyday Payments in Europe: Payment Services Directive (PSD2) enables Everyday Payments in Europe to move to the next level", Accenture, acceso del 10 de octubre de 2016. https://www.accenture.com/il-en/insight-everyday-payments-europe

[4] Douglas Bonderut, "SMS Two-Factor Authentication: Time to Trash the Text?" *IBM Security Intelligence*, 28 de julio de 2016. https://securityintelligence.com/news/sms-two-factor-authentication-time-to-trash-the-text/

WGW03255-ESES-00