IBM Security

Thought Leadership White Paper

July 2015

Supporting European Internet Payment Security Guidelines

Gain automated and powerful fraud prevention capabilities with IBM Security Trusteer solutions

Contents

Executive summary

In 2013, the European Central Bank (ECB) *Recommendations For The Security of Internet Payments* issued numerous recommendations for European payment service providers (PSPs) to enhance online fraud prevention practices. These recommendations are more expansive and detailed, yet fundamentally similar to the US Federal Financial Institutions Examination Council (FFIEC) landmark guidance entitled *Authentication in an Internet Banking Environment*.

The following year, the European Banking Authority (EBA) published its *Final Guidelines on the Security of Internet Payments*, based on the ECB recommendations, to document consistent procedures for European PSPs. Additional guidelines from the EBA are expected once the updated Payment Services Directive (PSD2) is published in 2017 - 2018.

While many PSPs have implemented numerous fraud prevention technologies and approaches, they may need additional capabilities in risk analysis, malware protection, and authentication to meet the Internet payment security guidance set forth by the ECB and EBA. The guidance from both regulatory organizations also cover mobile payments conducted via the mobile web browser, but for now exclude payments conducted via mobile applications.

This document discusses how IBM® Security Trusteer® solutions can help PSPs achieve effective and sustainable fraud prevention in alignment with the following guidance from the ECB and EBA:

- Risk assessment (guidance No. 2)
- Risk control and mitigation (guidance No. 4)
- Strong customer authentication (guidance No. 7)
- Enrolment for, and provision of, authentication tools and/or software delivered to the customer (guidance No. 8)
- Log-in attempts, session time-out, validity of authentication (guidance No. 9)
- Transaction monitoring (guidance No. 10)
- Customer education and communication (guidance No. 12)

Building effective and sustainable online banking fraud prevention

The Internet payment security guidance from the ECB and the EBA place the responsibility on PSPs to continually assess the risk associated with their payment operations and implement risk mitigation measures that are commensurate with the assessed risk.

As a result, while the documents outline a set of minimum expectations, they do not require PSPs to adhere to suggested technologies and programs outlined in the guidance. Ultimately, each organization has to implement the means it deems appropriate to mitigate its assessed risk. PSPs, however, will have to demonstrate how approaches different from those recommended provide an equivalent or superior security posture.

How can IBM help?

Since 2006, Trusteer has delivered a holistic cybercrime prevention platform that helps provide another layer of protection for organizations against financial fraud and data breaches. Based on the accumulated experience with hundreds of financial institutions worldwide, IBM has helped PSPs achieve effective and sustainable fraud prevention capabilities that aim to mitigate different online threats, such as phishing and malware attacks, in alignment with Internet banking security regulations, and in a cost-effective manner.

Through worldwide threat intelligence gathered from more than 270 million endpoints, expert research and development, and dynamic technology delivered via a Software-as-a-Service (SaaS) model, IBM can rapidly discover, analyze and provide another layer of protection for organizations and their customers against new threats as they emerge.

ECB/EBA Guidance	*How can IBM Security solutions help?*
Risk assessment	✓
Risk control and mitigation	✓
Strong customer authentication	✓
Enrolment for, and provisioning of, authentication tools and/or software delivered to the customer	✓
Log-in attempts, session time-out, validity of authentication	✓
Transaction monitoring	✓
Customer education and communication	✓

Through its work, IBM has identified the following fundamental approaches to support European Internet service payment guidelines for risk assessment (guidance No. 2); risk control and mitigation (guidance No 4); strong customer authentication (guidance No. 7); enrolment and provisioning of strong authentication tools (guidance No. 8); log-in attempts, session time-out, validity of authentication (guidance No. 9); transaction monitoring (guidance No. 10); and customer education and communication (guidance No. 12):

1. **Utilize real-time, intelligence-based risk assessment**. Early detection of changes in the threat landscape is essential to maintaining an effective risk assessment process and adapting defenses that can help to protect customers against online payment fraud.

2. **Layer security for online banking and payments fraud defense in depth**. By using multiple layers of security on the endpoint and web applications, it is possible to achieve powerful and flexible protection. Endpoint security provides another layer of defense, intelligence and remediation capabilities. Clientless malware detection provides instant coverage of end user systems and lower deployment impact.

3. **Extend protections to the customer device**. Malware has been able to bypass most security controls during the past several years. Preempting malware from infecting the endpoint and attacking the browser or the web application can help prevent fraud from occurring.

4. **Detect transaction anomalies early**. Early detection and prevention of malware attacks helps reduce the number of suspicious transactions that fraud and support teams must handle, and the resulting operational costs and staffing requirements.

5. **Minimize end user impact**. The balance of security, usability and interoperability helps facilitate end user adoption and minimizes the impact on day-to-day workflows without compromising security.

6. **Minimize deployment, management and operational costs to address guidelines on time and on budget**. Fraud prevention solutions should deploy quickly and require minimal intervention and ongoing maintenance from fraud, risk and support organizations.

7. **Team with a proven online banking fraud prevention provider**. Ultimately, fighting fraud is a team effort. Financial services institutions should select providers based on their ability to augment their staff with the expertise and capabilities to sustain an effective defense against cybercriminals.

Considerations when evaluating solutions

PSPs must consider multiple requirements when evaluating the deployment of online banking and payments fraud prevention and detection solutions to address the European Internet payment security guidance. Importantly, PSPs should evaluate a solution's deployment costs, management complexity and potential customer impact.

The following sections provide an overview of the fundamental approaches for effective and sustainable online banking fraud prevention, and compare IBM Security Trusteer solutions with other security control methods.

Gaining real-time, intelligence-based risk assessment

One of the core principals of current EU-wide guidance (guidance No. 2) is for providers to conduct continual **risk assessments**, and to adapt their security controls to address changes in the threat landscape. The ECB recommendations state that providers should "*perform specific assessments of the risks associated with providing internet payment services, which should be regularly updated in line with the evolution of internet security threats and fraud mechanisms.*"[1]

The EBA reiterates this guidance, writing that "*PSPs [payment service providers] should carry out and document thorough risk assessments with regard to the security of internet payments and related services, both prior to establishing the service(s) and regularly thereafter.*"[2]

Approaches

Risk assessment represents a considerable challenge to many organizations. Fraud and security teams gather threat intelligence from various sources to understand the threats that target their region, industry and specific institution, and to determine if their controls adequately address them.

IBM can help PSPs address the guidance for continual risk assessment. Threat intelligence, gathered from approximately 270 million endpoints, helps continually detect new threats and propagates crime logic (i.e., attack tactics) information to the Trusteer cloud. This threat intelligence is also used to help build new countermeasures, which are sent to Trusteer solutions to help update defenses.

IBM Security experts leverage this threat intelligence across multiple financial institutions using advanced data mining and analysis tools to identify new crime logic. PSPs can also monitor endpoint security health, risks, and adoption and usage of Trusteer endpoint protection layers. They can respond to alerts about specific risks by suspending transactions, taking down phishing sites, re-credentialing end users and remediating malware from infected endpoints.

Trusteer solutions use this information to provide organizations with:

- Real-time alerts
- Ongoing reporting (delivered through a Trusteer Management Application™ console)
- Automatic updates to Trusteer solutions to help ensure that the defenses are updated regularly

Summary: Threat research is necessary to meet the ECB and EBA guidance for ongoing risk assessment. PSPs that cannot conduct their own threat research, should team with a company like IBM that has a dedicated, global fraud prevention network and the process, people and expertise to perform continual risk assessment.

Layering security for online banking fraud defense in depth

The need for layered security is emphasized in current European Internet payment security guidance, and is considered a fundamental best practice in online banking and payments fraud prevention. In the preamble to the guidance for **risk control and mitigation** (guidance No. 4), the regulators specifically call out that security measures “*should incorporate multiple layers of security defences, where the failure of one line of defence is caught by the next line of defence (‘defence in depth’)*.”[1,2]

Approaches

Some approaches use profiling to identify fraudulent transactions. Due to the statistical nature of these approaches, false negatives and false positives frequently occur. Cybercriminals take many steps to perform fraudulent transactions “under the radar” of this security layer, exhibiting as many characteristics of normal, customer-generated transactions as possible.

Other endpoint security approaches focus on isolation of the online banking session from malware. However, as seen in recent attacks, once a host is infected with malware, it is possible to attack any security layer executing on the infected machine. Virtualization-based, browser solutions are no exception, and are susceptible to memory injections into their processes executing on the underlying host.

IBM offers multiple protection layers delivered through the following complementary product offerings:

- **The IBM Security Trusteer Rapport® solution** helps prevent malware and phishing attacks that represent the root cause of most financial fraud. It also helps PSPs maximize protection of their customers through removal and remediation of existing detected infections.
- **The IBM Security Trusteer Pinpoint Criminal Detection™ solution** provides evidence-based detection of fraudsters and account takeover attempts by combining traditional device IDs, geolocation and transactional modeling, and critical fraud indicators, such as phishing attacks, malware infections, credentials compromise and advanced evasion methods.

- **The IBM Security Trusteer Pinpoint Malware Detection™ Advanced Edition solution** provides real-time alerts to the PSP if the accessing device is infected with live Man-in-the-Browser malware while determining both the nature of the threat and the potential risk.
- **The IBM Security Trusteer Mobile SDK solution** provides a dedicated security library for mobile platforms that can be embedded in PSP's proprietary mobile banking and e-commerce applications to help detect compromised and vulnerable devices while generating a persistent device ID.
- **The IBM Security Trusteer Mobile Browser solution**, which is based on the Trusteer Mobile SDK, is a security-enabled browser application that allows safe access to online banking applications. It performs device status checking and provides information about malware and other possible security threats.

Client-based protection against advanced threats

The Trusteer Rapport solution incorporates several protection layers while helping to:

- **Protect against Man-in-the-Browser and Man-in-the-Middle attacks**. The Trusteer Rapport solution essentially locks down the browser. By doing so, it helps prevent malicious web page injection designed to social engineer victims into surrendering personal information or approving fraudulent transactions. It also helps block Man-in-the-Middle attacks by validating online banking IP addresses and confirming that SSL certificates belong to the genuine site.
- **Protect against credentials and personal information theft**. The Trusteer Rapport solution helps prevent login credential and personal information theft used to perpetrate account takeover and cross-channel fraud. It disables key logging and screen capturing attempts on sensitive application pages, such as the login and money transfer pages.
- **Prevent malware infection and remove existing malware**. Once installed, the Trusteer Rapport solution removes existing financial malware from end users' machines and helps prevent future infections by helping to stop attempts to exploit browser vulnerabilities and install malware on the endpoint. The solution provides a simple way for fraud and support teams to remediate threats on endpoints and resume safe online banking.
- **Stop phishing of login credentials and payment card data**. The Trusteer Rapport solution helps prevent credential and payment card data theft by detecting suspected phishing sites by a protected end user. The solution alerts the end user of a possible phishing attempt to help prevent data loss. Trusteer experts verify, in near-real time, that the site is in fact malicious. The site is added to the Trusteer Rapport black list to help prevent other end users from being phished. The PSP is notified to allow timely takedown and user re-credential.

Clientless detection of fraudulent activity

The Trusteer Pinpoint Malware Detection Advanced Edition solution helps to detect malware infections by detecting malware footprints on endpoints accessing an online banking site. The solution identifies the specific malware kit, the targeted PSPs and the attack type (e.g., credential theft, automated fraudulent transactions, etc.). PSPs can use the detection information to help protect against fraud by changing the application flow, elevating risk scores in risk engines, manually reviewing infected transactions, and optionally removing the malware with the Trusteer Rapport solution. Malware detection is performed in real time without requiring software installation on the endpoint. It is transparent to the end user and has no impact on application response time, as the endpoint analysis occurs in parallel with the banking session.

The Trusteer Pinpoint Criminal Detection solution helps protect websites against account takeover and fraudulent transactions by combining traditional device IDs, geolocation and transactional modeling, and critical fraud indicators. It provides several layers of protections including:

- **Transaction anomaly detection**. The Trusteer Pinpoint Criminal Detection solution correlates big data to link events across time, users and activities, phishing, malware and other high-risk indicators to provide more accurate "evidence-based" fraud detection than traditional anomaly detection approaches.
- **Complex device fingerprinting**. By matching new and spoofed device fingerprints, phishing incidents and malware-infected account access history, the Trusteer Pinpoint Criminal Detection solution can help to identify account takeover attempts, minimize customer burden and eliminate IT overhead.

- **Identification of phishing incidents in real time**. The solution also helps to identify, in real time, phishing incidents and related stolen credentials, and notifies the PSP. End users can be immediately re-credentialed by the PSPs to block the fraudster's access to a victim's account. Phishing site takedown can be initiated while the Trusteer Pinpoint Criminal Detection solution continues to provide a layer of protection against phishing attempts.
- **Login anomaly detection**. The Trusteer Pinpoint Criminal Detection solution looks for device anomalies (such as attempts to hide browser or operating system information), navigation anomalies, and even device-to-user anomalies (such as one device accessing numerous accounts). The solution can detect remote access tools, including Remote Desktop Protocol (RDP), VNC, Copilot, LogMeIn, WebEx, and more.

Mobile fraud risk prevention

The Trusteer Mobile SDK and Trusteer Mobile Browser solutions provide several layers of protections.

For example, the Trusteer Mobile SDK solution provides a dedicated security library for supported Apple iOS and Google Android platforms. The library can be embedded in the PSP's proprietary mobile banking and e-commerce applications and can help detect compromised and vulnerable devices, generate persistent device IDs, augment certificate authority security, and provide enhanced active protection for rooted or jailbroken mobile devices.

The Trusteer Mobile Browser solution, based on the Trusteer Mobile SDK solution, can help to:

- **Protect mobile web access**. Online banking customers can use the Trusteer Mobile Browser solution to access websites, while PSPs can confirm that their websites are only accessed via the Trusteer Mobile Browser solution. Whenever a protected PSP's website is accessed, a comprehensive security posture assessment is performed on the mobile device. The Trusteer Mobile Browser solution collects mobile device risk factors and sends these to the PSP's website and to the Trusteer Pinpoint Criminal Detection solution (to the extent deployed by the PSP), where they are used for mobile risk assessment.
- **Alert end users of device security risks**. End users using/running the Trusteer Mobile Browser solution can view the security status of their mobile devices through a dedicated dashboard. Indications of malware infection, unsecure Wi-Fi connections and other security risks are identified. The end user can mitigate these risks by following step-by-step remediation guidance provided by the Trusteer Mobile Browser application.
- **Protect end users from fake websites**. The Trusteer Mobile Browser solution also helps protect against pharming attacks. By validating both the IP address and the SSL certificate when a protected website is accessed, both session hijacking (Man-in-the-Middle) and redirection attacks can be prevented.

Summary: Since over time security measures can be compromised, PSPs should implement solutions that incorporate multiple security layers.

IBM offers multiple protection layers. The Trusteer Rapport solution forms the first layer that helps protect end user devices against malware infection and attacks on client applications, such as the web browser. Trusteer Pinpoint™ solutions create a second set of layers that helps detect high-risk devices and sessions, and phishing attempts. And the Trusteer mobile solutions provide a third layer that helps specifically address mobile web access.

Combined, Trusteer cybercrime prevention solutions can help PSPs effectively meet the European regulatory guidance for layered security.

Extending protections to the customer device

As a best practice for risk control and mitigation, European regulators recommend that PSPs provide "*security tools (e.g., devices and/or customized browsers, properly secured) to protect the customer interface against unlawful use or attacks (e.g. 'man in the browser' attacks)*."[1,2] (ECB 4.1 BP, EBA BP2)

The regulators warn against the primary enabler of online fraud—Man-in-the-Browser malware. The guidance also discusses the need to confirm **strong customer authentication** technologies are tamper resistant (ECB recommendation 7; EBA best practice 8).

Approaches

Cybercriminals have developed multiple techniques for bypassing strong authentication technologies, many of which employ a malware-based attack. For example, cybercriminals have used social engineering to fool end users into downloading SMS forwarders to mobile devices so the PSP's SMS one-time password (OTP) can be intercepted by the fraudster and used to authenticate fraudulent transactions.

In other attacks, malware is used to inject fraudulent transactions into fully authenticated, valid online banking sessions, while hiding the transaction and the resulting account balance information from the end user.

Trusteer cybercrime prevention solutions focus on the end user device as the first line of defense for online transactions, as the user endpoint has traditionally been considered the weak link in the Internet banking security chain. With Trusteer solutions, the protection layer is extended out beyond the walls of the PSP to the customer's desktop or mobile device, where, without the end user's knowledge, fraudulent transactions are initiated and user credentials are stolen.

Current EU-wide guidance regarding **enrolment and provisioning of strong authentication tools** further highlights that "*the enrolment for and provision of authentication tools and/or payment-related software delivered to the customer takes place in a safe and trusted environment*," and recommends that PSPs account for "the possible risks arising from devices that are not under the PSP's control."[1,2] (Guidance No. 8)

Trusteer solutions can help secure the endpoint during the authentication enrollment process by confirming a malware-free environment. IBM Security Trusteer employs multiple solutions working "behind the scenes," not requiring any input or interaction with the end user.

For example, the Trusteer Rapport solution helps protect the end user device from advanced information stealing malware. The Trusteer Pinpoint Malware Detection solution alerts PSPs when any supported device attempting to access the protected PSP's website contains active Man-in-the-Browser malware.[3] The Trusteer Pinpoint Criminal Detection solution collects information to generate a complex device fingerprint, profile user behavior, tag fraudster devices, help detect device spoofing, and help identify access with compromised credentials—all this in an aim to identify fraudulent account access. Additionally, the Trusteer Mobile SDK solution identifies device risk factors for securing authentication via mobile devices.

Summary: The end user device represents a weak link in the fraud prevention security chain. Extending defenses to the customer endpoint to help prevent and detect malware and phishing, as well as device and session anomalies helps provide a "front line" of defense that is invoked prior to a fraudulent transaction being initiated. The earlier the fraud attempts are identified and prevented, the less costly it is to the PSP in terms of customer impact, internal resources, and regulatory scrutiny.

Detecting transaction anomalies, including fraudulent log-in attempts, early

The European Internet payment security guidance for transaction monitoring (guidance No. 10) states that PSPs "*should use fraud detection and prevention systems to identify suspicious transactions before the PSP finally authorizes transactions.*"[1,2] The guidance also state "*such systems should also be able to detect signs of malware infection in the session (e.g., via script versus human validation) and known fraud scenarios.*"[1,2] (ECB 10.1 KC, EBA 10.1)

Since the root cause of most fraud loss is due to malware, preventing it from infecting the customer's machine and tampering with or initiating fraudulent transactions, is critical to preventing fraud.

Approaches

Some approaches to fraud prevention focus on identifying anomalous transactions. With these approaches, detection typically occurs after a transaction is submitted, but hopefully before funds are withdrawn from the account. Due to the statistical nature of these approaches, many false positives (a genuine transaction mistakenly identified as suspected fraud) are generated.

Fraud teams often struggle to effectively review the large number of anomalous transactions and may have to contact account holders to validate the transaction. Genuine transactions can be denied and some fraudulent activity can bypass the security controls.

The Trusteer Pinpoint Criminal Detection solution provides another layer of protection for Internet payment security against account takeover and fraudulent transactions. When an end user accesses a PSP's protected site, device and session attributes are remotely analyzed. This information is used to generate a complex device fingerprint, profile user behavior, tag fraudster devices, help detect device spoofing, and help identify access with compromised credentials.

Optionally, the Trusteer Pinpoint Criminal Detection solution can inspect transactions for known mule accounts and suspicious events, such as transaction sums or new payees added after a phishing event, among others. The solution correlates this data in real-time with other data sources such as real-time malware infection and phishing incidents, as well as information from the Trusteer Rapport endpoint solution (to the extent deployed) and other PSP's data feeds to help identify fraudulent account access.

The Trusteer Rapport endpoint solution helps prevent the initial infection that is the first step in the attack life cycle. If malware already resides on the machine, it can be stopped from attacking the browser and other key services, a key component of setting up the attack.

In addition to addressing transaction anomalies, the guidance also highlights the need to address **log-in attempts, session time-out, and validity of authentication via time and log-in limits.** (Guidance No. 9)

The Trusteer Pinpoint Criminal Detection solution leverages the context of a transaction ("log-in" information in this case) and provides the PSP with a definitive recommended action. This translates to a dynamic "max number of log-in" attempts that is adjusted for each customer session, improving the overall security of the environment.

Summary: Effectively containing fraud losses is best achieved by stopping malware from generating a fraudulent transaction. Trusteer solutions deliver transaction anomaly prevention tools that are based on intelligence from hundreds of organizations worldwide as outlined in the ECB and EBA guidance.

Delivering customer education and communication

European regulators emphasize the need for ongoing customer education and communication, recommending that PSPs "*communicate with their customers in such a way as to reassure them of the authenticity of the messages received.*"[1,2] (Guidance No. 12)

The Trusteer Rapport solution provides visible feedback to the end user about the protection status including warning on bad practices (e.g., when the customer navigates to a phishing site or attempts to submit credentials to other risky sites).

Likewise, with the Trusteer Mobile Browser solution end users can view the security status of their mobile devices, including indications of malware infection and unsecure Wi-Fi connections, through a dedicated dashboard.

Summary: By providing visible feedback directly to the end user, the Trusteer Rapport and Trusteer Mobile Browser solutions reinforce security awareness and alert end users of the advanced technology protections in place.

Minimizing end user impact

Online banking fraud prevention is a balancing act of security, transparency, usability and interoperability. Server-side solutions offer transparency, but often lack visibility into endpoint malware, the root cause of much fraud.

An important component of the recommendation for **transaction monitoring** is that PSPs "*perform any transaction screening and evaluation procedures within an appropriate time period, in order not to unduly delay the initiation and/or execution of the payment service concerned.*"[1,2] (ECB 10.4 KC, EBA 10.3)

Another important consideration of the European Internet payment security guidance is that when a potentially fraudulent payment transaction is blocked, the PSP should "*maintain the block for as short a time as possible until the security issues have been resolved*."[1,2] (ECB 10.5 KC, EBA 10.4)

Approaches

While specific timeframes are not provided, the intention of this guidance is to minimize the negative end user impact often associated with more basic fraud prevention solutions.

Some endpoint solutions necessitate that end users change the way they access web applications to reduce exposure. The impact of these solutions on end users acceptance and adoption of fraud prevention is substantial.

The Trusteer Rapport solution allows end users to continue using their PC of choice (Windows or Mac based[3]) and the commercial browser of choice (e.g., Internet Explorer, Firefox, Chrome or Safari). It is designed to operate transparently to the end user wherever possible so as to not interfere with their experience. At the same time, the solution helps protect customers from potentially risky operations, such as reusing their banking credentials on third party sites or entering their credentials on a phishing site.

Summary: To facilitate end user adoption of fraud prevention solutions, the impact on day-to-day workflows should be minimized. End users often find ways to stop using proposed security controls when their productivity is affected. The Trusteer Rapport solution has minimal impact on end user experience, helping to drive rapid adoption.

Minimizing deployment, management and operational costs

Implementation costs and complexity vary dramatically among different fraud detection and prevention products.

Approaches

During initial deployment, some solutions require substantial effort to establish and sustain a statistical baseline for normal end user activity. Once established, fraud teams often have to pursue a large number of potential fraud cases that are based on deviations from the profile, many of which are often false positives.

When fraud losses occur or fraudulent transactions are detected, PSPs often find the removal of malware to be a complex and daunting task.

Other approaches entail the distribution of hardware devices or complex software to end users (e.g., handheld PIN authentication or OTP generators). These deployments incur shipping, tracking and provisioning costs; cumbersome and complex update processes; and logistics overhead when devices have to be replaced due to loss or malfunction.

End users and PSP support teams may face the task of restoring endpoints to a "clean" state following a malware-driven fraud attempt. Often, end users have no choice but to format their computer or restore the operating system to its factory settings. Both approaches are highly disruptive.

Trusteer solutions deliver rapid time-to-value through the following capabilities:

- **Minimal false positives.** Trusteer solutions help detect malware's underlying crime logic to provide more accurate (not statistically generated) fraud detection. With minimal false positives, the operational costs associated with manual reviews and customer outreach is significantly reduced.
- **Remediation and malware removal.** The Trusteer Rapport solution can automate the removal of detected malware.
- **Scalable to retail and business channels.** Trusteer solutions help protect both retail and business online banking customers and do not require that PSPs patch together multiple technologies—a process that can create redundancies and management overhead.
- **Support of the end user environment.** Trusteer solutions allow end users to use their browser of choice (e.g., Internet Explorer, Firefox, Chrome and Safari), their PC platform (e.g., Windows or Mac[3]), and remote desktops (local, hosted and shared virtual machines).
- **No changes to end user workflow and third party applications.** No change in the use of third party applications, or modification to existing workflows are needed with the Trusteer Rapport solution and Trusteer Pinpoint solutions.

- **Vendor-managed client deployment and dedicated customer support:** PSPs often do not have the staff and skill set needed to successfully manage, deploy and provide ongoing end user support for new fraud prevention solutions. IBM automatically maintains its services to provide clients with an ongoing layer of protection against new threats. Trusteer Pinpoint solutions require a small change to the PSP's protected online application and can be easily integrated with the PSP's fraud prevention processes. The Trusteer Rapport solution is offered to end users during login through an IBM-provided "splash" message that enables opt-in or mandatory deployment. End users receive IBM's dedicated 24x7 support to address any technical questions they may have during installation or when using the product.

Summary: IBM can help PSPs address European Internet payment security guidance on time and on budget by allowing for quick deployment, and minimizing the rollout and support requirement from both PSP staff and end users alike. Malware removal and remediation capabilities help detected infected end users to quickly restore their systems to a clean state so their productivity is not affected. Software updates, when necessary, are typically pushed automatically from the Trusteer cloud to minimize user impact and help ensure protections adapt to new detected threats.

Teaming with a proven online banking fraud prevention provider

Teaming with a proven service provider can help PSPs to more efficiently address the ECB and EBA guidance, and provide another protection layer against fraud. Important considerations include the provider's global customer footprint and operational track record to demonstrate that it can effectively detect changes in the threat landscape, analyze them and sustain the effectiveness of its security controls over time.

Summary: By teaming with IBM, PSPs can benefit from years of experience servicing hundreds of financial institutions and more than 270 million endpoints, and a demonstrated ability to deliver sustainable fraud prevention over time.

Conclusion

Hackers often study end user and account behavior before attacking their targets, and have become adept at beating security controls, such as risk-based controls and strong authentication mechanisms. Because of this, static security controls have not been effective at stopping online banking fraud.

IBM can help PSPs address core ECB and EBA guidance for sustainable Internet payment security.

- IBM cybercrime researchers can help PSPs to address the ECB and EBA guidance for continual **risk assessment**.
- Coupling the Trusteer Rapport solution and Trusteer Mobile endpoint protection layers with Trusteer Pinpoint clientless detection layers enables organizations to address **layered security**.
- Real-time threat intelligence that continually adapts the security layers addresses the guidance for **risk control and mitigation**.
- Trusteer Rapport and Trusteer Pinpoint solutions form a comprehensive **transaction monitoring** solution that can help block and remove detected malware on the device, detecting malware-infected devices and sessions, and providing definitive recommendations regarding **log-in attempts, session time-out and validity of authentication**. These are fundamental capabilities that can add another layer in helping stop fraudulent transactions before they are submitted.
- By providing a first line of defense at the endpoint, Trusteer solutions can also confirm **the enrolment and provisioning of strong authentication tools** occurs in a malware-free environment, and can provide another layer of protection against malware-based attacks that would otherwise bypass **strong authentication** technologies.
- PSPs deploying the Trusteer Rapport solution can provide visible feedback directly to end users for improved **customer education and communication**.

Finally, Trusteer solutions deliver effective and cost-efficient security controls, not hindered by poor usability, limited platform support, long deployment processes and late detection of fraudulent transactions.

For more information

To learn more about IBM Security Trusteer solutions, please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/security

For more information about the European Central Bank (ECB) *Recommendations For The Security of Internet Payments*, visit: https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf

For more information about the European Banking Authority (EBA) *Final guidelines on the security of internet payments*, visit: https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+%28Guidelines+on+the+security+of+internet+payments%29.pdf

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

[1] The European Central Bank (ECB) *Recommendations For The Security Of Internet Payments* (2013). Retrieved from: https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf

[2] The European Banking Authority (EBA) *Final guidelines on the security of internet payments* (December 19, 2014). Retrieved from: https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+%28Guidelines+on+the+security+of+internet+payments%29.pdf

[3] Please refer to the following IBM Security Trusteer support page for a full list of supported platforms: https://www.trusteer.com/support/supported-platforms

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
July 2015

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

♻ Please Recycle