

Meeting FFIEC Guidance and Cutting Costs with Automated Fraud Prevention

White Paper

Table of Contents

Executive Summary	3
Key Requirements for Effective and Sustainable Online Banking Fraud Prevention Solution to Meet FFIEC requirements	3
Overview	4
#1 Layered security provides online banking fraud defense in depth	4
#2 Real-time, intelligence-based risk assessment	6
#3 Rapid adaptation to evolving threats	7
#4 Transaction Anomaly Prevention first	8
#5 Minimize end user impact: balance security, usability and interoperability	9
#6 Meet FFIEC requirements on time and on budget by minimizing deployment, management and operational cost	9
#7 Proven online banking fraud prevention partner	11
Summary	11
About Trusteer	12

Executive Summary

The 2011 FFIEC¹ supplement states that “controls implemented in conformance with the guidance several years ago [the 2005 original Guidance] have become less effective” and clarifies that “malware can compromise some of the most robust online” security controls. Unmistakably, what led to the release of the FFIEC supplement was the introduction of advanced malware that has created an increasingly hostile online banking environment. Sophisticated malware has become the primary attack tool used by online banking fraudsters to execute account takeover, steal credentials and personal information, and initiate fraudulent transactions. To address emerging threats the FFIEC requires organizations to continuously perform “risk assessments as new information becomes available”, “adjust control mechanisms as appropriate in response to changing threats” and “implement a layered approach to security”. Consequently, financial organizations need to select solutions that are able to identify emerging threats, address their impact and apply layered security that can quickly adapt to the ever changing threat landscape.

Trusteer has been protecting customers against online banking fraud since 2006. Based on our accumulated experience with hundreds of financial institutions (FI's), and millions of protected endpoints, we have identified key controls that are required to meet the FFIEC guidance and prevent fraud in a cost effective manner.

This document discusses how to achieve effective and sustainable online banking fraud prevention in accordance with FFIEC guidelines using the Trusteer Cybercrime Prevention Architecture.

Key Requirements for Effective and Sustainable Online Banking Fraud Prevention Solution to Meet FFIEC requirements

- **#1 Layered security provides online banking fraud defense in depth:** by using multiple layers of security on the endpoint and the web applications it is possible to achieve a powerful and flexible protection. Endpoint security provides prevention, intelligence and remediation capabilities and clientless malware detection provides instant coverage of all end users and lower deployment impact.
- **#2 Real-time, intelligence-based risk assessment:** as noted in the FFIEC guidance, malware has been able to bypass virtually all security controls over the past 5 years. Early detection of changes in the threat landscape is essential to maintaining an effective risk assessment process and adapting defenses that protect customers against online banking fraud.
- **#3 Rapid adaptation against evolving threats:** since all security controls are attacked by malware, they must be able to adapt to new attack vectors to maintain their effectiveness.

¹ FFIEC-Supplement to Authentication in an Internet Banking Environment June 2011

- **#4 Transaction Anomaly Prevention first:** preventing malware from infecting the endpoint and attacking the browser or the web application will prevent fraud from ever occurring. Early detection and prevention of malware attacks also 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:** balance security, usability and interoperability: to ensure end users adopt fraud prevention measures, the impact on their day-to-day workflow must be minimized without compromising security.
- **#6 Meet FFIEC requirements on time and on budget by minimizing deployment, management and operational costs:** Fraud prevention solutions should deploy quickly and require minimal intervention and ongoing maintenance from the fraud, risk and support organizations.
- **#7 Proven online banking fraud prevention partner:** Ultimately, fighting fraud is a team effort. Any partner must augment the FI's staff with the expertise and capabilities to help sustain an effective defense against cybercriminals.

Overview

When looking at the deployment of an online banking fraud prevention solution, financial institutions often have to consider multiple requirements. Beyond the core requirement of effective fraud prevention to meet FFIEC guidelines, there is a need to address deployment costs, management complexity and customer impact. In the following pages we will review some of these requirements and compare and contrast the Trusteer solution and other various security control approaches.

#1 Layered security provides online banking fraud defense in depth

Layered security is an FFIEC requirement and a fundamental best practice in online banking fraud prevention. Certain approaches use profiling to identify fraudulent transactions. Due to the statistical nature of these approaches, false negatives (missed fraud) are likely to occur. Cybercriminals take many steps to ensure fraudulent transactions “fly 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. As was proven many times over the past few years, once a host is infected with malware, it is possible to attack any security layer which executes on the infected machine. Virtualization-based, browser solutions are no exception, and are susceptible to memory injections into their processes executing on the underlying host².

² See Trusteer white paper - Virtual Browsers: Caveat Emptor

Trusteer Cybercrime Protection Architecture offers multiple protection layers delivered through two complementing product offerings:

- **Trusteer Rapport** prevents financial malware from infecting endpoints, secures the browser against tampering and data theft, provides automated remediation and blocks phishing attacks.
- **Trusteer Pinpoint** provides clientless detection of fraudulent activity, identifying malware infected web sessions, and phishing attacks.

Trusteer Rapport Layers

- **Secures against Man-in-the-Browser and Man-in-the-Middle attacks**

Trusteer Rapport locks down the browser to prevent malicious web page injection designed to social engineer victims into surrendering personal information or approving fraudulent transactions. Trusteer Rapport blocks Man-in-the-Middle attacks by validating online banking IP addresses and SSL certificates belong to the genuine site.

- **Protects against credentials and personal information theft**

Trusteer Rapport prevents login credential and personal information theft used to perpetrate account takeover and cross-channel fraud. It disables key logging and screen capturing attempts of sensitive application pages such as the login and money transfer pages.

- **Prevents malware infection, removes existing malware**

Once installed, Trusteer Rapport removes existing financial malware from end-users machines and prevents future infections by stopping attempts to exploit browser vulnerabilities and install malware on the endpoint. Trusteer Rapport provides a simple way for fraud and support teams to remediate threats on endpoints and resume safe online banking.

- **Stops phishing of login credentials and payment card data**

Trusteer Rapport prevents credential and payment card data theft by detecting suspected phishing sites on first access by a protected user. Trusteer Rapport alerts the user of a possible phishing attempt to prevent data loss. Trusteer Cybercrime Intelligence Center experts verify, in near real-time, that the site is in fact malicious. The site is added to Trusteer Rapport's black list to prevent other users from being phished. The financial institution is notified to allow timely takedown and user recredential.

Trusteer Pinpoint Layers

- **Detects malware infection**

Trusteer Pinpoint detects malware footprint on endpoints accessing an online banking site. It identifies the specific malware kit, the targeted banks and the attack type (e.g. credential theft, automated fraudulent transactions). Banks use detection information to prevent fraud by changing the application flow, elevating risk scores in risk engines, manually reviewing infected transactions and cleaning infection with Trusteer Rapport. Malware detection is performed in real-time without requiring software installation on the endpoint, is totally transparent to the end user and has no impact on application response time.

- **Identifies phishing incidents in real-time**

Trusteer Pinpoint for Phishing Detection identifies, in real time, phishing incidents and related stolen credentials and notifies the financial institution. The user is immediately re-credentialed by the financial institution to block the fraudster's access to the victim's account. Phishing site takedown is initiated while Trusteer Pinpoint continues to protect against phishing attempts from the site.

Bottom line: No security solution can rely on a single layer of protection. And, over time any security measure can be compromised. Trusteer Rapport forms the first set of layers that secures end user devices against malware infection and attacks on client applications such as the Web browser. Trusteer Pinpoint creates a second set of layers that detects high risk devices and sessions, and phishing attempts. Combined, the Trusteer Cybercrime Prevention Architecture enables FIs to meet and exceed the FFIEC requirement for Layered Security.

#2 Real-time, intelligence-based risk assessment

As noted in the new 2011 FFIEC guidance, the effectiveness of security measures used by financial institutions (FIs) has eroded since the FFIEC issued its previous guidance in 2005. This realization has prompted the FFIEC to require FIs to conduct continuous risk assessment and adapt their security controls to address changes in the threat landscape.

Risk assessment represents a considerable challenge to many organizations. Fraud and security teams must gather threats intelligence from various sources, understand the **threats that target their region, industry and specific institution**, and determine if their controls are adequately addressing them. Performing threat analysis requires technology and expertise that are not available to many FIs.

Trusteer Cybercrime Intelligence allows FIs to meet the FFIEC requirement for continuous risk assessment. A network of tens of millions of Trusteer protected endpoints continuously detect new threats and propagate Crime Logic (i.e. attack tactics) information to the Trusteer Cybercrime Intelligence cloud.

Trusteer Cybercrime Intelligence Center experts leverage threat intelligence across multiple customers and use advanced data mining and analysis tools to identify new Crime Logic. Financial institutions can also monitor endpoint security health and risks, adoption and usage of Trusteer endpoint protection layers. FIs can respond to alerts about specific risks by suspending transactions, taking down phishing sites, recredentialing users and removing malware from infected endpoints.



Figure 1: Trusteer's Cybercrime Intelligence cloud

Bottom line: Threat research is required to meet the FFIEC requirement for continuous risk assessment. FIs that can't conduct their own threat research, should partner with a vendor like Trusteer that has a dedicated, global fraud prevention network and the process, people and expertise to perform continuous risk assessment.

#3 Rapid adaptation to evolving threats

The mirror FFIEC requirement of risk assessment is **adaptive protection** (FFIEC guideline to "adjust control mechanisms as appropriate in response to changing threats"). Once a new threat or a new attack vector is identified through the risk assessment process, a countermeasure must be rapidly developed and deployed across all protected applications and users. FIs should assume that the security controls they implemented will be attacked by malware and must be able to respond the "day after" the latest and greatest security innovation is bypassed.

Trusteer's Adaptive Protection process quickly turns zero-day attacks into known Crime Logic and automatically integrates new Crime Logic into Trusteer's products (Trusteer Rapport and Trusteer Pinpoint) to promptly detect and block these attacks on protected endpoints.

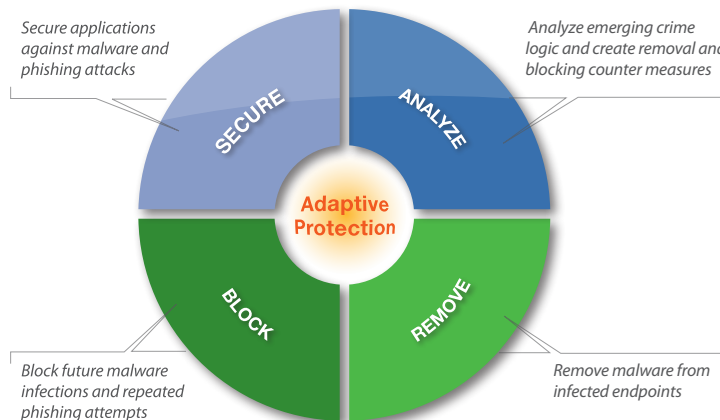


Figure 2: Trusteer's Adaptive Protection Process

Bottom line: whether they protect the endpoint or the server, any security control can be compromised over time. Trusteer delivers a timely, automated and scalable adaptive process to update security controls against emerging threats. Trusteer Rapport and Trusteer Pinpoint update process is transparent to end users and requires no involvement from the FI's IT and fraud teams.

#4 Transaction Anomaly Prevention first

The FFIEC guidance states that financial institutions "should include processes designed to detect anomalies and **effectively respond** to suspicious or anomalous activity related to....initial login and authentication and.. initiation of electronic transactions.". Since the root cause of most fraud losses is malware, preventing malware from infecting the customer's machine and tampering with or initiating fraudulent transactions, is critical to preventing fraud.

Certain approaches to fraud prevention focus on identifying anomalous transactions. Detection occurs after a transaction is submitted but 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 struggle to effectively review the large number of anomalous transactions, possibly requiring reaching out to accountholders to validate the transaction. Eventually, many genuine transactions are denied and some fraudulent activity is able to bypass the security controls.

Trusteer Rapport endpoint software prevents the initial infection that is the first step in the attack life cycle. If the 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. Trusteer Pinpoint's clientless malware detection can directly identify anomalous risky activity at login before an actual fraud attempt occurs, and feed risk data into risk engines or the online banking application. Adjusted transaction risk

score can be used to restrict access to functions such as adding a payee or transferring money. In both cases, Trusteer directly detects and protect against malware on the endpoint, preventing anomalous transactions from ever been submitted.

Bottom line: effectively containing fraud losses favors stopping malware from ever generating a fraudulent transaction. Trusteer delivers transaction anomaly prevention which specifically addresses the FFIEC requirement to “**effectively respond** to suspicious or anomalous activity”.

#5 Minimize end user impact: balance security, usability and interoperability

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

Some endpoint solutions require the end users to 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.

Trusteer Rapport allows users to continue using their PCs (Windows or Macs), familiar commercial browser of choice (i.e., Internet Explorer, Firefox, Chrome or Safari) and be able to print and use 3rd party applications. Trusteer Rapport protection is provided in the background with minimal user interaction, as most users are unable to make decisions about threats and risks and will likely make the wrong choice if prompted.

Bottom line: To ensure end users adopt fraud prevention solutions, the impact on their day-to-day workflow should be minimized. If end users’ well-being is downplayed for perceived better security, they will find ways to stop using the proposed security controls. Trusteer Rapport has minimal impact on end user experience driving faster and wider adoption.

#6 Meet FFIEC requirements on time and on budget by minimizing deployment, management and operational cost

Fraud prevention products should be simple to deploy and operate. While this is a universal truth, actual implementation costs and complexity vary dramatically between different products.

During initial deployment, some solutions require substantial effort to establish and sustain a statistical base line for normal user activity. Once established, fraud teams must pursuit a large number of possible fraud cases that are based on deviations from the profile, most of which are false positives. Ultimately, when fraud losses occur or fraudulent transactions are detected, FIs face very limited options for remediation, as the removal of malware is a complex and daunting task.

Other approaches require distribution of hardware devices or complex software to end users. These deployments incur shipping, tracking and provisioning costs, cumbersome and complex update processes and logistics overhead when devices have to be replaced if lost or malfunction. End users and FIs support team 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 hard drives, or restore the operating system to its factory settings. Both approaches are highly disruptive

Trusteer delivers quick Time-to-Value:

- **No false positives:** Trusteer detects malware’s underlining crime logic to provide accurate (not statistically generated) fraud detection. With no false positives the operational costs associated with manual reviews and customer outreach is significantly reduced.
- **Remediation and malware removal:** Trusteer Rapport offers an automated way of removing malware.
- **Scalable to all channels (retail and business):** Trusteer protects retail and business online banking end users. Eliminating the need to patch together multiple technologies creating redundancies and management overhead.
- **Supports the end user environment:** Trusteer allows end users to use their browser of choice (e.g. IE, Firefox, Chrome and Safari), their PC platform (e.g. All flavors of Windows and Mac), and remote desktops (local, hosted and shared virtual machines).
- **No changes to end users workflow and 3rd party applications:** Trusteer Rapport and Pinpoint require no change in the use of 3rd party applications, or modification to existing workflows.
- **Vendor Managed Client Deployment and Dedicated Customer Support:** in most cases, FIs do not have the required staff and skill set to successfully manage, deploy and provide ongoing end user support to new fraud prevention solutions. Trusteer automatically maintains its service to ensure all customers are continuously protected against new threats. Trusteer Pinpoint cloud-based service requires a small change to the online banking application and can be easily integrated with the FI’s fraud prevention processes. Trusteer Rapport is offered to end-users during login through a Trusteer-provided “splash” message enabling opt-in or mandatory deployment and end users receive dedicated 24X7 support to address any technical questions they may have during installation or when using the product.

Bottom line: Trusteer enables FIs to meet FFIEC guidelines on time and on budget by allowing for quick deployment, and minimizing the rollout and support requirement from the FI and the end users. Malware removal and remediation capability enables infected users to quickly restore their system to a clean state so their productivity is not affected.

#7 Proven online banking fraud prevention partner

FIs must partner with a service provider that can enable them to achieve compliance and effectively prevent fraud. The chosen vendor must have the 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.

Bottom line: By partnering with Trusteer, FIs benefit from accumulate experience servicing hundreds of FIs and tens of millions of protected end users and a demonstrated ability to deliver sustainable fraud prevention over a long period of time.

Summary

According to a 2011 Gartner survey³ of 76 U.S. banks, malware-driven attacks became the crime web-fraud detection vendors had to beat in 2011. Established vendors came up relatively short in stopping malware-driven attacks as some hackers studied user and account behavior before pouncing on their targets proving adept at beating security controls such as risk based and strong authentication. Clearly, when selecting an online-banking fraud prevention solution it is imperative to understand that no **static** security control can remain effective at stopping online banking fraud. Trusteer allows FIs to meet the core FFIEC requirement for sustainable online banking fraud prevention. Coupling Trusteer Rapport endpoint protection layers and Trusteer Pinpoint clientless detection layers, enables organization to address **layered security**. Real-time threat intelligence that continuously adapts the security layers addresses the FFIEC requirement for **continuous risk assessment** and **adjusting security controls** respectively. Trusteer Rapport and Trusteer Pinpoint form a complete **transaction anomaly prevention** solution, stopping fraudulent transactions before they are submitted by blocking and removing malware on the device, and detecting malware infected devices and sessions. Furthermore, Trusteer delivers effective and cost-efficient security controls, not hindered by poor usability, limited platform support, long deployment processes and late detection of fraudulent transactions.

³ Magic Quadrant for Web Fraud Detection 19 April 2011

About Trusteer

Trusteer is the leading provider of cybercrime prevention solutions that protect organizations against financial fraud and data breaches. Hundreds of organizations and millions of end users rely on Trusteer to protect their computers and mobile devices from online threats that are invisible to legacy security solutions. Trusteer's Cybercrime Prevention Architecture combines multi-layer security software and real-time threat intelligence to defeat zero-day malware and phishing attacks, and help organizations meet regulatory compliance requirements. Leading organizations such as HSBC, Santander, The Royal Bank of Scotland, SunTrust and Fifth Third are among Trusteer's clients.

For more information visit: www.trusteer.com.