Entrust®
Securing Digital Identities & Information

EntrustSecurity
@Entrust

FFIEC Compliance Guide

Implementing strong authentication, real-time transaction verification and layered security techniques as long-term solutions for financial institutions

Get this White Paper

Entrust.com
1-888-690-2424
Entrust@Entrust.com

Contents

Introduction

With every new data breach revealed or costly identity-theft case reported, consumer confidence in the security of online banking erodes. This loss of confidence in online services can have a direct impact on the ability of financial institutions to reduce costs and increase efficiency through the online-banking channel.

Today, financial institutions offering Internet-based and mobile-banking services face increasing pressure to provide enhanced consumer protection against phishing, sophisticated malware (e.g., man-in-the-browser attacks, ZeuS, SpyEye, Ice IX) and other fraudulent activities.

First issued in 2005, the Federal Financial Institutions Examination Council's (FFIEC) guidance for financial institutions took a strong stance in support of the deployment of stronger authentication methods, as well as fraud detection techniques, to protect customer identities and information during online-banking transactions.

Updated in June 2011, the FFIEC's "Authentication in an Internet Banking Environment" guidance recognizes the significant advances in criminal threats — both in sophistication and sheer frequency. The supplement provides comprehensive guidelines to help stop advanced attacks that target the identities and transactions of consumers and business-banking customers. This guidance suggests that affected organizations:

- **Drive Better Risk Assessment**
- **Adopt Strong Authentication Standards**
- **Push Toward Layered Security**
- **Explore Advanced Authentication Techniques**
- **Enhance Customer Awareness & Education**

Complying with the FFIEC guidance requires financial institutions to thoroughly review their online activities and conduct risk assessments to determine the level of authentication and fraud detection required. Institutions must then develop and deploy additional online safeguards and systems as identified by the assessment.

The updated FFIEC guidelines are a necessary response to the increased number of identity fraud cases and continued threats from phishing, malware and man-in-the-browser attacks. But earning the approval of the FFIEC is just one milestone in a continuing effort to bolster consumer confidence. Security threats will continue to evolve and financial institutions should invest in security platforms that provide the flexibility to implement new approaches and adapt to future challenges.

This document presents an overview of security options — with emphasis on strong authentication, fraud detection and general layered security — that can help address the FFIEC requirements now and protect consumers over the long term.

To read the entire FFIEC guidance, please **visit entrust.com/ffiec**.

> *"… financial institutions offering Internet-based and mobile-banking services face increasing pressure to provide enhanced consumer protection against phishing, sophisticated malware and other fraudulent activities."*

A Dynamic Threat Landscape

First, it's important to understand the reality of these fast-evolving dangers — financial institutions are constantly targeted by advanced malware threats that easily circumvent many traditional security safeguards.

Instead of phishing attacks that lead to fake websites designed to harvest usernames and passwords, the techniques are now more sophisticated and are effective against previously deployed defenses. Whereas once such attacks were the domain of amateur hackers, sophisticated cybercrime groups have emerged as online fraud leaders, targeting consumer- and commercial-banking users alike.

The United States now has the highest concentration of websites that host the ZeuS crimeware package. And the merger of the ZeuS crimeware toolkit and its one-time rival SpyEye has not only brought together two crimeware toolkits, but also two different bot networks.[1]

But traditional phishing attacks continue to be a problem. While the number of these attacks is still down from the peak in August 2009, the number of domain names and URLs used for phishing attacks has increased, and widespread database breaches have made it easy for criminals to obtain user credentials such as passwords and personal information.

Not an option in 2005, the proliferation of mobile devices now offer financial institutions an opportunity to leverage the device itself to strengthen both online and mobile security, while addressing customer demand for extended mobile-banking services.

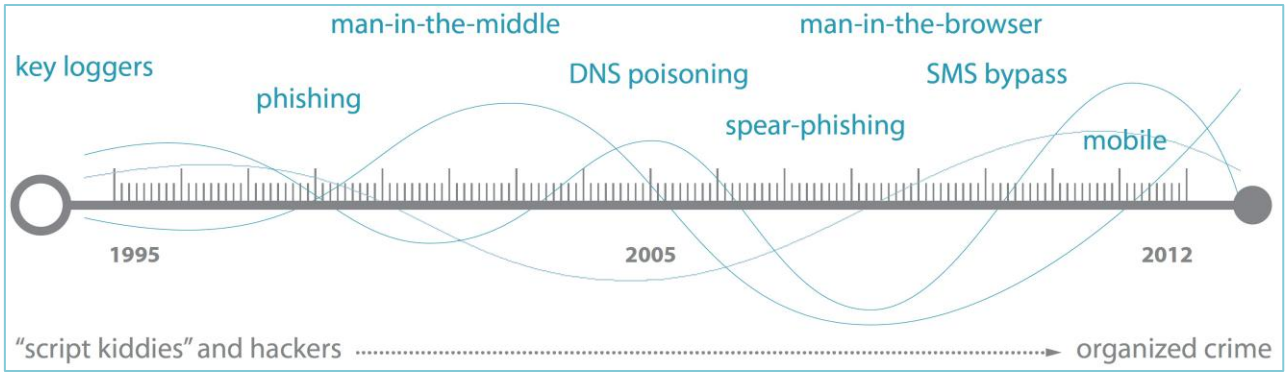

Figure 1: Organized crime groups are innovative and fast-moving, developing advanced malware and fraud techniques that easily defeat outdated or single-layer security schemes.

[1] "Enhanced SpyEye Trojan Poses New Threat," Mathew Schwartz, Information Week, February 8, 2011.

While there are many safeguards deployed within financial institutions, criminals are evolving their techniques rapidly. Phishing, smishing and spear-phishing attacks are now designed to deploy malware, which takes over users' browsers and mobile devices to execute malicious transactions.[2] The malware also is crafted to avoid detection by antivirus tools.

Understanding the FFIEC Recommendations

Since the original guidance in 2005, financial institutions have typically taken one of two different approaches:

1) Spend resources constantly, deploying "band-aids" that do just enough to achieve basic compliance

2) Invest in long-term solutions that enable them to be nimble and adjust security controls to keep pace with evolving threats

While meeting compliance guidelines is necessary for financial institutions, it is important not to lose sight of the real objective of the FFIEC guidelines — keeping customer transactions secure and restoring consumer confidence in the online-banking channel, which holds such great promise for both consumers and retail banks.

This section breaks down each of the five primary FFIEC recommendations outlined in the introduction. This systematic approach gives financial institutions a better understanding of the mandate, whether or not their specific organization is in compliance, and then offers solution options to help implement effective security control systems.

[2] A spear-phishing attack is a highly targeted form of phishing, using specific messages and information tailored to a particular user or small user group.

Drive Better Risk Assessment

Developing a strategic vision for securing online relationships with customers means making security choices that will address today's requirements and can adapt to help meet tomorrow's challenges.

To realize this vision, it is necessary to carefully assess an institution's online transactions and the level of risk presented by each type of transaction or user group. The FFIEC advises financial institutions to carefully examine their current online practices and develop effective risk mitigation strategies for these varied transaction types. In addition, the guidance outlines that risk assessments should be reviewed whenever new online services are offered — at least every 12 months.

Further, specific attributes of a financial institution's online services should be examined during the risk-assessment process. Financial institutions need to consider which types of customers they are securing; the capability of their current transaction methods; information sensitivity and existing security; the ease of use and impact on the customer experience; the overall volume of transactions completed; and how mobile devices are interacting with banking environments. Examples of these considerations include:

Customer Type	Retail, high-net-worth or commercial clients
Information Sensitivity	Customer information and privacy regulations
Ease of Use	Relative importance and impact on customer experience
Transaction Volume	Number of transactions and impact on security choices
Mobile Landscape	Types of mobile transactions, devices and services
Transaction Capability	ACH payments, wire transfers, loan origination, control of account administrative functions, etc.

The risk assessment should also review the possible impacts of a problem for specific services by considering the potential damage to an institution's brand and reputation, as well as the financial loss or liability of fraud attacks. The unauthorized release of sensitive information and data, and the ramifications of compliance failure, should be evaluated during the risk-assessment process.

Once completed, a risk assessment will outline the specific services and products that have an increased likelihood of being compromised and will result in a more severe impact if there are fraudulent activities. Potential impacts and particular services can be mapped to specific security levels.

For example, a bank may determine that all services conducted with corporate accounts have a higher potential impact and require strong/step-up authentication, a fraud detection solution or a combination of several solutions as part of a comprehensive layered security approach.

The report may identify circumstances where less security is acceptable (e.g., corporate customers can review transaction histories and account information with single-factor authentication, but will need to use a higher level of security when they want to initiate transactions).

Adopt Strong Authentication Standards

While the 2005 guidance stated that usernames and passwords weren't enough, today's threats require even stronger means of authentication, particularly for high-risk transactions (e.g., ACH and wire transfers for commercial transactions). That's where strong authentication, deployed in layers, is effective against the most advanced malware threats.

Financial institutions have known for some time that usernames and passwords alone are insufficiently effective protection for user accounts. Numerous other strong authentication techniques are available and address a wide range of threats that are still relevant.

Traditional two-factor authentication solutions such as one-time-passcode tokens, while continuing to be effective in layered scenarios, are no longer effective against sophisticated man-in-the-browser attacks when used as a lone security device.

Fortunately, a number of newer techniques provide effective protection against man-in-the-browser attacks, either through the use of a separate communication channel with the user, or by relying on advanced behavior-based fraud detection engines that can automatically detect transaction or website navigation anomalies in real-time.

Push Toward Layered Security

Multiple layers of process or controls help defend against identity attacks, including advanced malware. If one security layer fails, subsequent barriers are in place to thwart an attack. Step-up security options can include, as an example, out-of-band authentication and advanced transaction verification.

All leading analyst firms that specialize in banking security, including TowerGroup[3] , openly state that no single authentication or traditional fraud detection solution can stop advanced malware or sophisticated attacks on banks and other financial institutions.

It's the layering of several different, complementary security technologies — strong authentication, behavioral fraud detection, out-of-band transaction verification, mobile authentication, extended validation SSL digital certificates — that provide the best method of protecting customer identities and transactions in a banking environment. Several of these are explained in further detail later in this document.

Explore Advanced Authentication Techniques

As online fraud attacks increase in sophistication, so does the innovation in authentication technology required to stop the attacks in the consumer space. Financial institutions should explore, for example, advanced techniques like dynamic device authentication solutions including one-time session cookies and digital fingerprints, rather than broadly used static device cookie-based approaches.

But fighting online fraud isn't a "checkmark" fix. It's a continuously evolving investment in technology, process, human resources and innovation. The moment an organization becomes complacent with their security infrastructure, they open themselves up for attack.

By exploring and investing in new and advanced authentication techniques, financial institutions are able to better keep pace with the sophisticated fraud schemes leveraged by well-funded criminal groups.

The more advanced authentication techniques include mobile out-of-band transaction verification, advanced mobile authentication solutions and behavioral fraud detection. The latter monitors transaction and session navigation attributes in real-time to detect anomalies and stop transactions before they execute.

> *"Financial institutions must implement layered security approaches that integrate multiple fraud detection methods to maximize the system's effectiveness in detecting and preventing both known and unknown fraud techniques."*[3]
>
> — ***George Tubin***
> ***Sr. Research Director***
> ***TowerGroup***

[3] "US Business Banking Cybercrime Wave: Is 'Commercially Reasonable' Reasonable?" George Tubin & Susan Feinberg, TowerGroup, August 9, 2010.

Enhance Customer Awareness & Education

One of the most effective ways of fighting fraud is involving the customer as much as possible in the process. This is achieved via ongoing customer education, awareness and training — all to ensure everyone does their best to help protect and mitigate the effects on today's fraud threats.

Beyond education and awareness, the more a financial organization involves their customers in the fraud process itself, the more likely online fraud threats will be effectively thwarted.

For example, progressive banks are deploying effective security measures that automatically notify a customer when suspicious or high-risk transactions are in progress and require the customer to affirm that a given transaction is valid.

Key Considerations for Evaluating Security Solutions

When evaluating potential security solutions and vendor claims, specifically when in regards to FFIEC compliance, carefully consider the following criteria:

Invasiveness	No matter which security method or deployment plan is selected, the new security safeguards should not impose burdens or new hardware requirements on users, but rather leverage existing technology and interaction models that are natural and easy to use. Leveraging a customer's mobile device is a smart method to deploy strong security that is in line with the mobile-user paradigm of this day and age.
Cost-effectiveness	As future fraud threats are inevitable, the ongoing needs for authentication and fraud detection requirements are an unknown. Choose a platform-based approach that can help meet needs now and provides a proven architecture that can grow and change to meet new fraud threats over time.
Adaptability	As business demands change and innovative services are offered online, new security methods may be needed. Choose a full-featured platform that uses a multilayered approach as described in the FFIEC guidance.
Integration	Security solutions are just one part of a complex and multifaceted online system. Choose a platform that can effectively integrate with other security systems.
Security Expertise	Choose a company that is a proven security leader with a trusted reputation and focused dedication on identity-based security at its core.

Speed of Deployment

The FFIEC guidance demands an aggressive timetable (i.e., less than a calendar year). Choose a platform that can help meet current and long-term goals, and can be implemented quickly from a proven vendor with deployment experience.

Comprehensiveness

Look for solutions that offer a wide breadth of authentication options, deployment methods and fraud detection techniques. This is critical to provide the options to meet the needs of varied user communities (e.g., employees, retail banking, commercial banking, etc.) but also helps implement various layers of security controls to ensure the overall system is designed to adapt to various risk scenarios.

A product/vendor that simply offers a point solution or limited set of authentication options may help "band-aid" today's needs, but will not be able to adapt to new fraud threats and customer demands, leaving organizations with islands of technology solutions.

Mobile Innovation

Does the solution leverage the ubiquity of mobile devices to strengthen security for both mobile- and online-based transactions?

Can the solution use existing customer mobile devices for strong authentication or transaction verification? Select a platform that uses all available technology to properly safeguard customer identities and transactions.

Selecting the appropriate technology vendor to provide any security method can be daunting, especially if each is evaluated individually as a stand-alone system.

One key to assessing and selecting appropriate solutions is to examine security holistically — looking at all layers of security requirements as a single system with different capabilities for various services.

Smartly choose a platform that will deliver a range of multifactor authentication and fraud detection capabilities, as cornerstones to a comprehensive layered security environment, which can respond and adapt to future changes.

Introduction to Strong Authentication

The FFIEC guidance takes a firm stance on single-factor authentication: it is not enough to protect against current online account fraud and identity attacks. To understand the details of their position, and what it means in terms of required changes to current processes, a short review of authentication factors is helpful.

Authentication factors are independent methods of establishing identity and privileges. Factors simply ask and answer, “How do we know you are who you say you are?” Existing authentication methods can involve up to three factors:

Knowledge *something the user knows (password, PIN)*
Possession *something the user has (ATM card, smartcard)*
Attribute *something the user is (biometric such as fingerprint)*

In general, today’s banks are specifically relying on usernames/passwords and then possibly some form of knowledge-based authentication (e.g., question and answer, password replay, PIN). Online fraud and identity attacks are frequently the result of the exploitation of single-factor authentication or weak multifactor authentication schemes. Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods.

Adding factors of authentication can increase security and help limit vulnerability to identity attacks. Properly designed and implemented multifactor authentication methods are more reliable, are stronger fraud deterrents and can have varying levels of user impact.

But why don’t many banks deploy effective multifactor authentication today? Based on most financial institution’s innate ability to manage risk through business means, most have considered this level of security a low priority given the cost and resources required to manage and deploy multifactor solutions. In addition, traditional solutions have not always provided the flexibility and ease of use; banks have seen security as a necessary evil, rather than a means to build customer loyalty and competitive advantage in the marketplace.

Often, worries that users will find the process of authenticating with multiple factors complicated or intimidating have inhibited the use of multifactor solutions. But as risks increase, phishing and malware attacks continue to grow, and brands are impacted by breaches and fraud incidents, the true importance and necessity of strong, multilayered authentication becomes clear.

Independent of the FFIEC guidance, the issue of user acceptance must remain in the forefront of all authentication decisions. An effective strong authentication deployment must be easy to use and have customer acceptance — no matter how many or which factors are used. Determining which additional factors to use and how to implement them, with the least possible stress on users, requires a thorough assessment of risk and careful selection and planning.

Strong Authentication Methods

There are many diverse authentication methods, ranging from simple single-factor authentication in the form of usernames and passwords to sophisticated strong authentication mechanisms. Each method delivers a different balance point between cost, security and user complexity.

Core to an identity-based security approach, the wide variety of authentication options available today can help increase security for specific activities and user communities.

A number have proven to be very effective for strong authentication in banking environments, including:

- **Security grid cards**
- **Soft tokens (via SMS, mobile applications, etc.)**
- **Digital certificates**
- **Machine authentication (e.g., device profiling)**
- **Knowledge-based authentication**
- **Out-of-band authentication (via email, SMS, etc.)**
- **IP-geolocation**
- **Physical tokens (only when used in layered security schemes)**

These authentication methods, which have broad acceptance in the consumer market, are detailed on the following pages.

> *… the issue of user acceptance must remain in the forefront of all authentication decisions. An effective strong authentication deployment must be easy to use and have customer acceptance — no matter how many or which factors are used.*

Authenticator	Description
Physical Tokens	One of the first second-factor authentication options, tokens deliver strong authentication via a variety of form factors, including random-number one-time-passcode (OTP) tokens, USB tokens and even credit card-sized tokens. But as recent security breaches have proven, these are often ineffective when used in token-only security infrastructures. Physical tokens are, however, still valuable when used as single components within a more comprehensive layered security environment. Physical tokens traditionally have been relatively expensive to deploy, manage and maintain. New platform approaches to authentication have minimized management complexity and significantly reduced the price of OTP tokens to the $5 range.
Grid Cards	Security grid cards can provide strong second-factor protection using a grid card issued to each user. Users enter characters from the grid at login. Inexpensive to produce and deploy, and easy to use and support, these highly intuitive cards have a very high success rate in banking environments. Grid cards can be produced and distributed in a number of ways, including a credit card-like format in thin plastic, paper or deployed digitally to smartphones and mobile devices.
Soft Tokens	OTP software tokens can be generated on mobile devices or laptops, enabling organizations to leverage devices for strong authentication that are already used by online-banking customers. This is a convenient, cost-effective method of rolling out easy-to-use strong authentication to a broader base. While similar in nature to hard tokens from a security perspective, one distinct advantage is that the unique token security key — known commonly as a “seed file” — is generated locally on the mobile device rather than generated by the token manufacturer. The benefit is that there is not a global repository of seed files that can be breached as has been recently seen in the marketplace.
Digital Certificates	Digital certificates, such as those powered by a PKI, can also provide benefits of second-factor authentication, without having to deploy a physical OTP. Digital certificates provide an advantage of extensibility to other functions, beyond authentication, such as encryption and digital signatures.

Authenticator	Description
Machine Authentication/ Device Profiling	This non-invasive method of strengthening user authentication stores and validates a “fingerprint” of a registered machine. The fingerprint consists of a variety of elements gathered from the user’s machine such as the operating system, screen resolution, browser type or even IP address. The stored machine fingerprint is compared with information gathered from the machine when a user attempts to log in. This method does not require any user interaction beyond initially registering the machine and can be very cost effective to deploy. It is important to note, however, there are various approaches to machine authentication and the FFIEC guidance is clear on the ineffectiveness of static device cookies.
Knowledge-Based Authentication	This intuitive method of authentication uses challenge questions and answers to provide strong authentication. This enhances authentication without the need to deploy anything physical to the end-user.
Out-of-Band Authentication	Out-of-band user authentication leverages an independent means to communicate with the user beyond the primary communication channel. By using a different medium (e.g., smartphone, mobile device, email or SMS) an independent authentication challenge can be delivered to the user. Out-of-band user authentication can be a cost-effective, user-friendly option since existing devices, already owned by end-users, can be leveraged. This eliminates the need for the deployment of new or additional devices.
IP-Geolocation	Authenticated users can register locations where they frequently access the online-banking sites or services. During subsequent authentications, the server compares their current location data, including country, region, city, ISP, latitude and longitude, to those previously registered. Financial institutions only need to “step up” authentication when the values don’t match. Organizations can create blacklists of regions, countries or IPs based on fraud histories. They can even leverage an open fraud intelligence network to receive updated lists of known fraudulent IPs based on independent professional analysis.

Fraud Detection Overview

Online criminals repeatedly attempt to circumvent traditional authentication safeguards through phishing, malware and man-in-the-browser attacks. Fraud detection can add a much-needed layer of security for consumers and is an important element in any consumer protection strategy designed to help thwart today's online attacks.

A key advantage of using fraud detection to provide a second layer of security is the ability to be implemented quickly and without invasive impact to existing applications or the user experience.

There are many diverse fraud-monitoring methods, ranging from simple transaction values to complex Web navigation behavioral profiling. Each method delivers a different value in analyzing the transaction session for anomalies.

As part of an identity-based security approach, a platform supporting a wide variety of monitoring options can help increase security for specific activities and user communities. A number of these capabilities have proven to be very effective for fraud monitoring in banking environments, including:

- **"Front door" fraud analysis**
- **Transaction monitoring (individual user)**
- **Multi-user/cross-site monitoring**
- **Web navigation monitoring**
- **Alert management and workflow**
- **Reporting and forensics**

Fraud Detection Technique	Description
"Front Door" Analysis	"Front door" fraud monitoring includes a number of techniques to access anomalies and risk in the transaction when the user first accesses the system. Comprehensive systems will assess: • Device and IP address analysis and comparison against history, black lists and use of device/IP for other user accounts • Location-change assessment based on the time between various login sessions • Typical access time of day or day of week
Transaction Monitoring	Transaction monitoring can include various components — including individual user requests, or a combination of user requests — such as: • Large money transfers • Abnormal money transfers for individual users • Money transfers to new or risky destination accounts • Behavior indicative of account takeover such as changing contact address, executing high-value transaction, or changing mailing address and then ordering checks • Transaction velocity
Multi-user/Cross-Site Monitoring	While analyzing discrete transactions is important to detect potential fraud, criminals will often conduct a series of seemly "normal" transactions over time in an attempt to "fly under the radar" of a fraud detection system. For example, a user's credentials are unknowingly compromised and the criminal transfers $3,000 to an external bank account. This type of transaction would likely be considered "normal" and "low risk" and would not be blocked or require step-up authentication. However, if several users are conducting similar fund transfers, all to the same external account, this pattern of transaction activity should be flagged as potential fraud.

Fraud Detection Technique	Description
Web Navigation Monitoring	While monitoring traditional transaction values is important, progressive fraud attacks hijack a user's session and mask both the identity and often the behavior profile of the user. Therefore, it is critical that a fraud detection system analyze Web navigation patterns to detect MITB and MITM attacks. Typical techniques include: • HTML injection detection • Website navigation speed • Suspicious user agent strings • IP address changes mid-session • Unusual or impossible page navigation
Alert Management & Workflow	A fraud detection solution should provide monitoring and forensic tools to help institutions evaluate access patterns and study potentially new patterns of fraudulent behavior. Accordingly, a fraud detection solution must possess: • Powerful analytics engine to rapidly process the massive transaction volumes generated online • Real-time alert management interfaces for fraud analysts to triage and investigate suspected fraud • Easy-to-use dashboards • Workflow tools • Drill-down analysis • Summary reporting • Forensics and fraud team performance metrics

Entrust®
Securing Digital Identities & Information

Addressing FFIEC Guidance — Entrust Can Help

Entrust offers proven solutions to help organizations and financial institutions comply with FFIEC mandates. Entrust's comprehensive layered security approach — comprised of several proven security solutions — is cost-effective, simple to deploy and easy for end-users.

Solution					
Guidance	**Entrust IdentityGuard**	**Entrust IdentityGuard Mobile**	**Entrust Transaction Guard**	**Entrust EV Multi-Domain SSL Digital Certificates**	**Details**
Drive Better Risk Assessment	✓	✓	✓	✓	Understand how to detect and thwart threats, as well as analyze security breaches
Adopt Stronger Authentication Standards	✓	✓			Use stronger device authentication, including one-time cookies, to create more complex digital PC fingerprints; increase strength of challenge questions
Push Toward Layered Security	✓	✓	✓	✓	Enable use of different security functions at different points in a transaction process; if one is compromised another control is in place
Explore Advanced Fraud & Authentication Techniques for Effective Controls	✓	✓	✓		Consider innovative security controls, including anti-malware software for customers, transaction monitoring, anomaly detection and mobile transaction verification
Provide Technology Guidance for Compliance	✓	✓	✓	✓	Educate customers as to how and where they are protected within today's current fraud landscape

Entrust IdentityGuard — Software Authentication Platform

Much of the FFIEC guidance focuses on the adoption of strong authentication — for consumers and commercial banking use alike. Banks are directed to provide commercial customers with strong multifactor authentication.

It also requires financial institutions to adopt the use of stronger transparent authentication — such as session-based device authentication (e.g., one-time cookie or dynamic device authentication) — that is stronger than simple device identification.

Solution	FFIEC Requirement
Entrust IdentityGuard	Strong Authentication
	Layered Security
	Device identification using digital fingerprinting and dynamic cookies
	Flexible approaches to challenge question

Entrust IdentityGuard is a software authentication platform that enables banks to deploy a single authentication infrastructure capable of providing different types of multifactor authentication, depending upon the type of user, transaction or risk. The platform enables financial organizations to comply with the primary FFIEC guidelines.

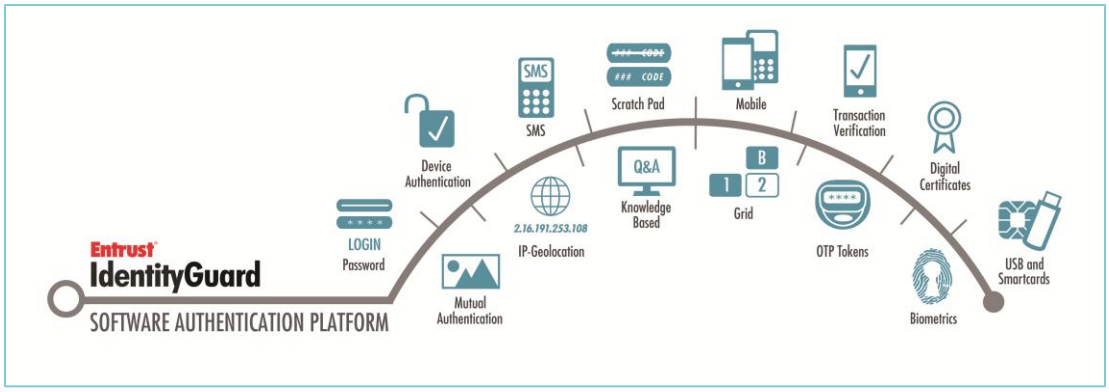

Figure 2: The award-wining Entrust IdentityGuard software authentication platform offers more authenticators than any solution on the market and is a key component in a comprehensive framework proven to stop malware and online fraud.

Entrust®
Securing Digital Identities & Information

Entrust IdentityGuard Mobile

Transaction Verification

FFIEC guidance requires banks to ensure systems are in place that thwart attacks with a layered security approach. In addition to providing a convenient, cost-effective approach for stronger authentication via soft tokens, Entrust IdentityGuard Mobile also enables out-of-band transaction verification with one of the most secure and user-friendly approaches on the marketplace today.

This simplicity helps users verify whether transaction integrity is intact or if some form of fraud attack has modified it. Transaction verification is a proven approach for banks to defeat many types of online and mobile malware threats.

Soft Tokens

Entrust's convenient mobile soft tokens are placed on mobile devices to serve as an authenticator to enterprise networks, applications and resources. During a transaction that requires authentication, a user is asked for the token's security code (i.e., one-time passcode) displayed within their application. A correct response grants secure access to the resource, application or network.

Device Certificates

By deploying digital certificates directly to mobile devices, organizations are able to authenticate the device before it connects to the network. Digital certificates deployed to mobile devices help organizations identify and authorize specific devices that are communicating with the corporate network, protecting access and enabling organizations to better leverage the business potential of mobile devices.

SMS OTP Tokens

By taking advantage of existing SMS technology, mobile devices can be leveraged as very flexible, convenient and low-cost methods for authentication. By deploying one-time passcodes (OTP) to a mobile device via SMS, organizations can dramatically reduce obstacles that once made traditional enterprise-wide deployment of physical OTP tokens impractical.

eGrid Authentication

Entrust's patented grid-based authentication is one of the most popular and easy-to-use methods of strong authentication.

As an eGrid authenticator, a unique image is stored on a mobile device that consists of numbers and/or characters in a row-column format. Upon login to a website or application, users are presented with a coordinate challenge and must respond with the information in the corresponding cells from the unique eGrid card they possess.

Entrust TransactionGuard — Real-Time Fraud Detection

Banks are now required to maintain systems capable of preventing fraud attacks and have the ability to analyze incidents that have occurred. The guidance specifically addresses security solutions effective in combating online fraud, including approaches that provide transaction monitoring and anomaly detection (i.e., software that detects transactions that may be inconsistent with established patterns of behavior).

Entrust TransactionGuard provides robust, real-time capabilities to protect against online fraud, and offers forensic capabilities to analyze ongoing and/or past transactions to identify potential fraudulent activity.

Solution	FFIEC Requirement
Entrust TransactionGuard	Login/"front door" fraud analysis
	Comprehensive in-session transaction anomaly detection
	Behavior profiling that builds a profile based on customer history
	IP analysis and blocking capabilities
	Web access behavior profiling capable of identifying compromised user devices (malware detection)
	Ability to monitor and alert on changes to administrative controls
	Forensics and reporting tools

EV Multi-Domain SSL Certificates — Website Security

Extended validation (EV) SSL digital certificates are the first line of defense in thwarting online fraud — particularly phishing attacks — by providing users with a strong indication that they are on a legitimate website.

Under the new guidance, organizations are required to provide these types of simple measures (e.g., visual clues) to help users easily understand easily if they are at risk during an online session.

Banks and financial institutions are also required to implement better education for their users. For example, visual clues, such as the green address bar provided by an EV SSL certificate, are a simple and effective way for banks to make users aware of risky or legitimate sites.

FFIEC Compliance & Beyond

The FFIEC guidance provides the banking community with a vision on how to improve overall security for online services. And when addressing the updated FFIEC requirements, financial institutions need to consider a multilayered, platform-based approach, consisting of strong authentication, fraud detection and SSL digital certificates, as a long-term strategy to protect consumers and restore confidence. But achieving FFIEC compliance is just the first step in the process of helping to maintain consumer confidence in online banking.

A strategic view of securing the online relationship with customers dictates using technology that will help satisfy today's needs, but also has the ability to extend to address tomorrow's obstacles, including the reality of multichannel communication (e.g., mobile, online, IVR). This approach can be effective in the face of yet-seen threats and can help accelerate the delivery of new online products and services by ensuring customer confidence.

Implementing a strategic plan should consist of working with strategic partners. Based on proven capabilities for more than 15 years and with 5,000 customers, Entrust is committed to providing its customers with solutions to broadly protect financial institutions and the online customer relationship.

To read the entire FFIEC guidance, please visit entrust.com/ffiec.

Entrust & You

More than ever, Entrust understands your organization's security pain points. Whether it's the protection of information, securing online customers, regulatory compliance or large-scale government projects, Entrust provides identity-based security solutions that are not only proven in real-world environments, but cost-effective in today's uncertain economic climate.

A trusted provider of identity-based security solutions, Entrust empowers governments, enterprises and financial institutions in more than 5,000 organizations spanning 85 countries. Entrust's award-winning software authentication platforms manage today's most secure identity credentials, addressing customer pain points for cloud and mobile security, physical and logical access, citizen eID initiatives, certificate management and SSL.

For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **entrust.com/ffiec**.

Company Facts

Website: www.entrust.com
Employees: 359
Customers: 5,000
Offices: 10 Globally

Headquarters

Three Lincoln Centre
5430 LBJ Freeway, Suite 1250
Dallas, Texas 75240

Sales

North America: 1-888-690-2424
EMEA: +44 (0) 118 953 3000
Email: entrust@entrust.com

follow us on twitter tweet