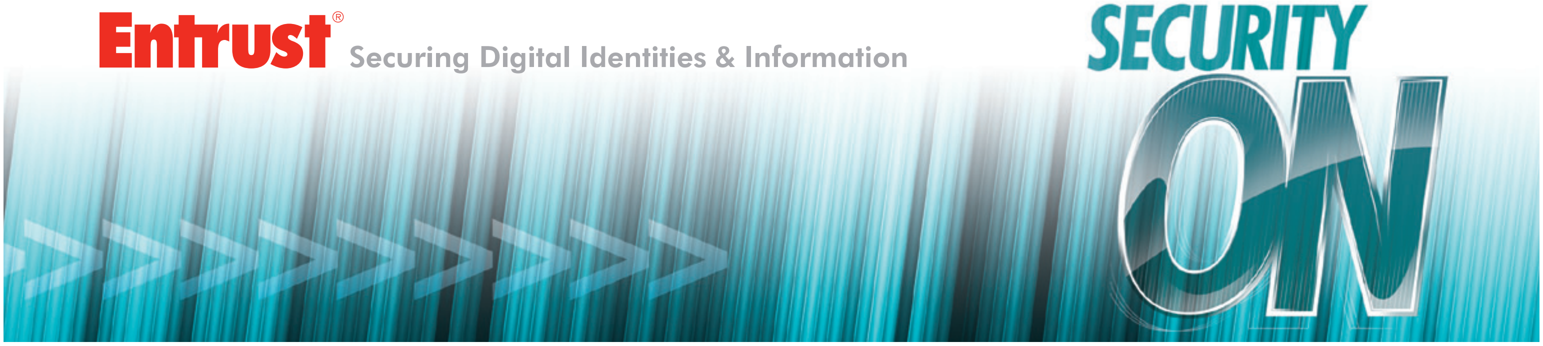
Entrust® Securing Digital Identities & Information



Complying with FFIEC Guidance

Proven Security Solutions for Financial Institutions

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

Like the original, the updated guidance is supported by all five members of the FFIEC, which is an interagency body in the United States that sets the principles and standards used for reporting and examining financial institutions.

Entrust provides the guidance, expertise and proven solutions to help banks and financial institutions comply with the FFIEC's latest requirements and recommendations.

To help organizations protect against a broad range of online and mobile threats, Entrust offers the broadest range of solutions to ensure that an effective balance of security, user experience and total project cost is achieved.

A New Focus

The original 2005 FFIEC guidance was a major impetus to the adoption of stronger authentication beyond standard username and password schemes.

But the growth of online threats, such as the ZeuS Trojan and man-in-the-browser attacks, coupled with the growing losses among business, served as the catalyst for the FFIEC to revisit those guidelines.

With a focus on the ongoing threats to customer- and business-banking transactions and respective identities, the FFIEC's updated guidance addresses the following areas of focus.

Who is Affected?

- Banks
- Thrifts
- Mortgage lenders
- Credit unions (and their non-functionally regulated operating subsidiaries)
- U.S. branches and agencies of foreign banks
- U.S. commercial-lending companies of foreign banks
- Creditors
- Any person or business* who arranges for the extension, renewal or continuation of credit

* In addition to banking institutions, retailers, utilities, car dealers and many other businesses are subject to this regulation.

Guidance & Recommendation

Drive Better Risk Assessment

Financial institutions require a better understanding of the sophisticated threats and their appropriate, timely response. This includes guidance for regular reviews by the banks of internal systems and the ability of these systems to detect and deal with fraud threats.

Adopt Stronger 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).

Push toward Layered Security

Multiple layers of process or controls have been proven to 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 out-of-band authentication and advanced transaction verification.

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 device authentication via one-time session cookies or stronger challenge questions.

Provide Technology Guidance for Compliance

The FFEIC now provides instruction on technology and solutions, particularly fraud detection platforms, which will be effective in meeting the new guidelines. This includes fraud transaction monitoring and/or anomaly detection software.

Entrust Enables FFIEC Compliance

Much like with the 2005 FFIEC guidelines, Entrust offers proven solutions to help organizations and financial institutions comply with the new mandates. Entrust's comprehensive security framework — comprised of several proven security solutions — is cost-effective, simple to deploy and easy for end-users.

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.

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.

Just one of the many authenticators supported by Entrust IdentityGuard, digital certificates can be deployed easily by Entrust Managed Services PKI — a simple, cost-effective hosted PKI offering. While providing a convenient authentication mechanism for users and devices, digital certificates also enable banks to tighten security processes within the institution and enhance security of internal systems.

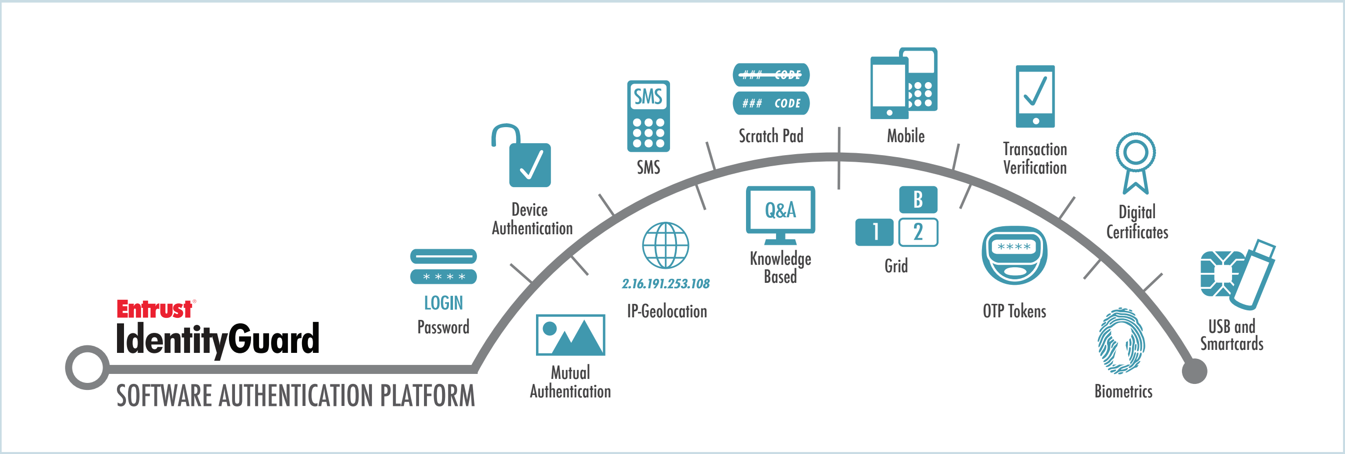
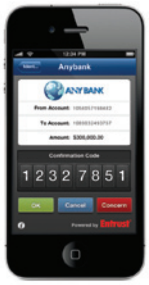


Figure 1: A software authentication platform enables financial institutions to select the right authenticator for each user or device based on risk, cost and/or transaction type.

Entrust IdentityGuard Mobile: Transaction Verification

The updated 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.


Anybank

ANYBANK

From Account: [illegible]

To Account: [illegible]

Amount: $300,000.00

Confirmation Code

1 2 3 2 7 8 5 1

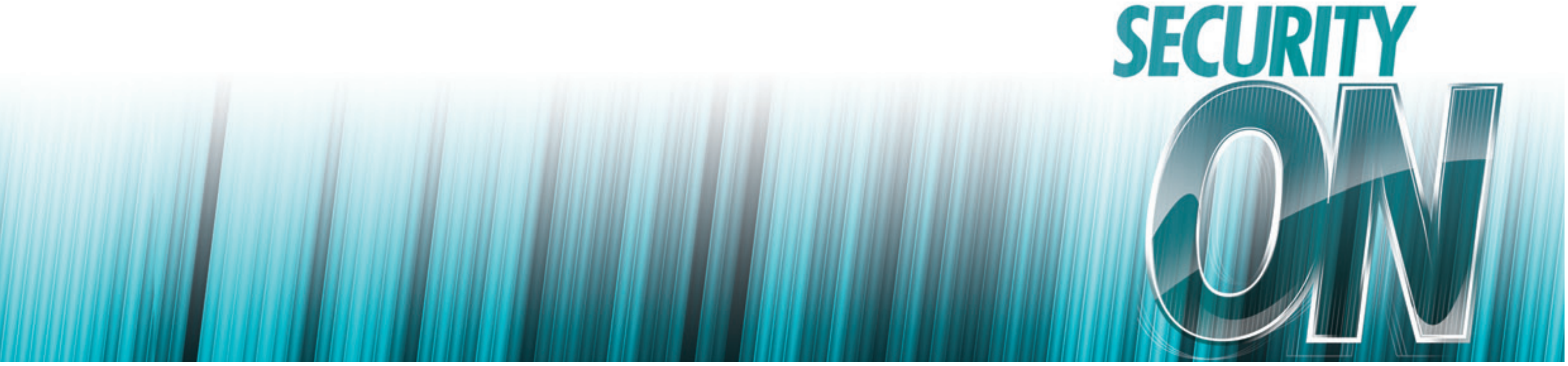
This helps users verify whether transaction integrity is intact or if it has been modified by some form of fraud attack. Transaction verification is a proven approach for banks to defeat many types of online and mobile malware threats.

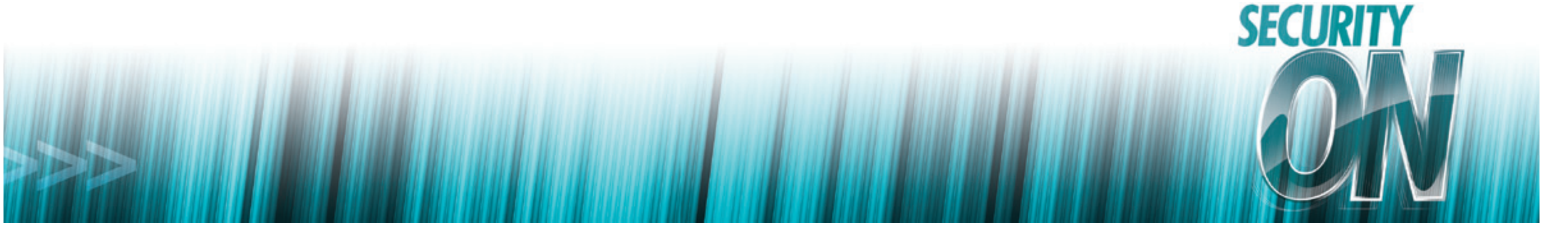
Entrust TransactionGuard: Real-Time Fraud Detection

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					
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 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.

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.

The smart choice for properly securing digital identities and information, Entrust solutions represent the right balance between affordability, expertise and service. For more information on how Entrust can help your organization comply with FFIEC guidelines, contact the Entrust representative in your area at **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, TX 75240 USA

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

About Entrust
A trusted provider of identity-based security solutions, Entrust secures 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 **www.entrust.com**.

Entrust® Securing Digital Identities & Information