PAYMENT SOLUTIONS

ProfitStars®

Securing Online Payments in the EPS Merchant and Partner Portals

sales@profitstars.com
877.827.7101
www.ProfitStars.com

Contents

Overview

Purpose

The Federal Financial Institutions Examination Council (FFIEC) holds financial institutions responsible for securing their online payment systems. As the provider behind those systems, however, ProfitStars believes a partnership between processors, financial institutions, and businesses is the best way to prevent fraud. By leveraging the combined expertise of system providers, bankers, and business clients, banks and credit unions can implement more effective security controls.

To that end, ProfitStars has produced this white paper as a means to:

- Help educate financial institutions regarding online payment security.
- Provide details about the robust security measures available today in the Enterprise Payment Solutions (EPS) product suite.
- Advise FIs regarding planned enhancements they can factor into their security roadmap.

While it touches on a wide range of information, this white paper is focused on current security measures available from EPS. ProfitStars is publishing this information to help financial institutions with their FFIEC-mandated risk assessments and subsequent layered security systems. This document does not address broader security issues, such as security measures available in EPS applications, mitigation methods not applicable to online payment systems, or techniques ProfitStars uses to secure its online data centers.

ProfitStars cannot prescribe the exact steps financial institutions must take to comply with FFIEC mandates, but it can and does offer a robust array of security tools to help those institutions combat the threats they identify in their risk assessments. This white paper provides information that will help financial institutions understand those tools and deploy them more effectively against the threats.

Regulatory Foundation

The financial services industry has been very focused on the FFIEC's supplemental guidance published in June 2011. Financial institutions should, however, be familiar with a much broader range of FFIEC publications.

When preparing this white paper, ProfitStars considered the following documents:

- *Authentication in an Internet Banking Environment* (August 2001)[1]
- *Authentication in an Internet Banking Environment – Update* (October 2005)[2]
- *Risk Management of Remote Deposit Capture* (January 2009)[3]
- *Supplement to Authentication in an Internet Banking Environment* (June 2011)[4]

These documents provide direction – sometimes specific, sometimes general – for financial institutions, detailing how they must secure their online banking systems. The requirements set forth in these publications include:

- The need for financial institutions to perform periodic risk assessments.
- The need for financial institutions to educate customers/members about fraud.
- The need for financial institutions to implement layered security systems.
- The need for financial institutions to mitigate fraud related to "high risk" transactions.

[1] See http://www.ffiec.gov/pdf/pr080801.pdf.

[2] See http://www.ffiec.gov/pdf/authentication_guidance.pdf.

[3] See http://www.ffiec.gov/pdf/pr011409_rdc_guidance.pdf.

[4] See http://www.ffiec.gov/pdf/auth-its-final%206-22-11%20(ffiec%20formated).pdf.

The FFIEC has defined "high risk transactions" as online events that transmit non-public consumer information or move funds between parties.

Because remotely deposited checks facilitate the movement of funds between parties, FFIEC guidelines specifically include them as high risk transactions.[5] Even so, the FFIEC's 2011 supplemental guidance focuses on outbound funds transfers (ACH credits and wire transfers) as the areas of greatest risk.

Customer/Member Education

The FFIEC guidance documents listed above contain recommendations for financial institutions regarding their role in educating their customers/members about fraud. While this white paper does not provide specific information to help financial institutions with these FFIEC-mandated customer education efforts, FIs must include this activity in their risk mitigation plans.

Threats

Understanding threats is a precursor to assessing risk. Accordingly, financial institutions must gain a working knowledge of current attack methods prior to producing a risk assessment.

While the attack details vary widely, payment system fraud can be divided into these categories:

- Trusted entity theft
- Account takeover
- Session manipulation

The following sections provide more information about each type of attack.

Trusted Entity Theft

Trusted entity theft is fraud committed by known users. For online corporate payment systems, trusted entity theft includes fraud committed by:

- Financial institution employees.
- Corporate customers/members and their employees.
- Consumers.

This type of fraud is committed by registered users who access the system with valid credentials. Online security measures are often focused on preventing access by illegitimate users. Since trusted entity theft involves fraud committed by legitimate users, it can be difficult to prevent.

Account Takeover

Account takeover occurs when an illegitimate user gains access to a customer's or member's funds. In recent years, the frequency of corporate account takeover has increased dramatically due to the exponential proliferation of credential-stealing malware.

Account takeover begins when fraudsters entice unsuspecting users to install malware. This is often accomplished through phishing attacks that deliver Trojan programs as attachments to email or text messages. In spear phishing attacks, fraudsters target specific users with bogus emails or text messages purporting to be from known businesses, or even from the financial institution itself. Once the user inadvertently installs the malicious program, it monitors system activity, captures credentials for online payment sites, and transmits those credentials to the fraudsters. Armed with valid credentials, illicit users then log in to the system and attempt to transmit funds to accounts controlled by the fraudsters.

[5] *Risk Management of Remote Deposit Capture*, FFIEC, January 2009, p.5, paragraph 1.

Because these fraudsters access the system with valid credentials, financial institutions must implement sophisticated mitigation techniques to prevent this type of attack.

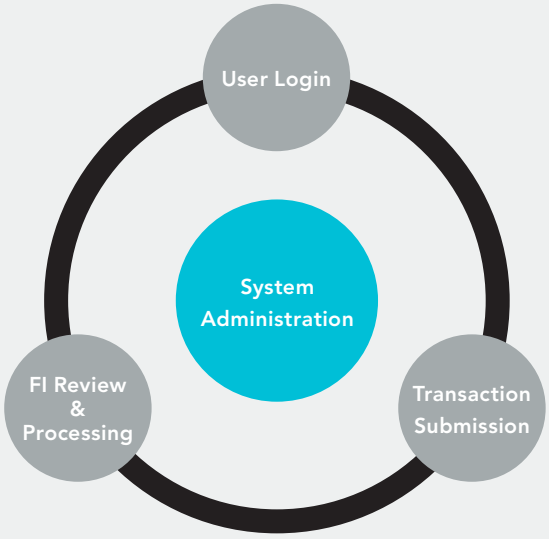
Session Manipulation

Session manipulation is a sophisticated attack where fraudsters gain control of an online session established by a valid user. Fraudsters then either launch a parallel fraudulent session or – even more insidious – alter the routing number and account number information on legitimate transactions to reroute them to fraudulent accounts.

Session manipulation attacks can be launched by fraudsters who establish themselves as a proxy. In this approach, referred to as a man-in-the-middle (MIM) attack, the fraudster inserts himself between the user and the online site in order to read or alter the information being transmitted between the two legitimate parties. Session manipulation can also be performed programmatically by malicious browser add-ons. In this approach, referred to as a man-in-the-browser (MIB) attack, illicit programs monitor online activity until sessions are established with targeted financial institutions. During those sessions, the malware will change account information for legitimate transactions, rerouting them to fraudulent accounts. Because these types of attacks "piggyback" onto sessions established by valid users, they can be difficult to identify and prevent.

The Transaction Process

The most recent FFIEC guidance requires that financial institutions place "different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of a different control."[6]



As a prerequisite for implementing layered security, financial institutions must understand the "transaction process." It may be beneficial for financial institutions to create a high-level flowchart depicting the transaction process for each type of online payment they facilitate.

ProfitStars divides the transaction process into four primary areas:

- User Login
- Transaction Submission
- FI Review and Processing
- System Administration

Financial institutions may find this an effective model around which to structure their risk assessment and the subsequent plan to address the threats they identify.

Layered Security

The FFIEC mandates that financial institutions mitigate online threats by implementing layered security. According to the FFIEC, layered security is characterized by these elements:[7]

- It uses multiple fraud prevention measures.
- Prevention measures are placed at different points in the transaction process.
- Prevention measures are deployed in a way that ensures weaknesses inherent in one measure will be compensated for by strong points in other measures.

[6] *Supplement to Authentication in an Internet Banking Environment*, June 2011, p. 4 paragraph 2.

[7] Ibid, p. 4, "Layered Security Programs."

The FFIEC's most recent guidance states that examiners will look for these specific components of a layered security system:

- Effective user authentication measures
- Methods to detect and respond to suspicious activity
- Administrative controls for profile and configuration changes

The most recent guidance also mentions other security methods, including:

- Dual authorization for transactions or configuration and/or profile changes.
- Out-of-band authentication during transaction initiation.
- "Positive pay" or debit blocks.
- Velocity controls and monetary user limits.
- Access controls based on IP address, the time of day and/or the day of the week.
- Transaction controls that restrict transfers only to pre-approved accounts.

In short, the FFIEC expects to see appropriate security measures from the list above deployed in various places in the transaction process in ways that address the threats identified in the financial institution's risk assessment.

EPS Merchant and Partner Portals Security Measures

This section of the white paper details the security measures available in the EPS Merchant and Partner Portals. This information is organized around the high-level view of the transaction process described in a previous section.

Some security features are available as part of the baseline EPS product suite. Other security measures may require the purchase of additional modules.

User Login Security Measures

Keeping illicit users out of the system is the first line of defense in a layered security system. Accordingly, user authentication is the security area most frequently referenced by the FFIEC. While the most recent guidance goes far beyond the topic of user authentication, it retains the title *Authentication in an Internet Banking Environment*. This shows the vital place authentication holds in a layered security approach.

EPS offers robust authentication options for financial institutions. By deploying some or all of these measures, financial institutions can create a layered security approach, even within the context of the user login phase of the transaction process.

Multifactor Authentication

Through ProfitStars' relationship with RSA®, the industry leader in user identification technology, the EPS product suite offers a range of multifactor authentication options.

RSA's Adaptive Authentication uses complex device identification[8] in conjunction with a wide range of other session information to identify anomalies in user login practices. If the estimated risk exceeds an established threshold, the user is challenged. This allows repeat users with known computers to gain access quickly, while incorporating challenges for higher risk logins.

The Adaptive Authentication service also leverages RSA's eFraud Network™. This network combines security information from RSA clients across the globe that helps identify fraudulent entities and block access from suspicious sites. By leveraging the eFraud Network, EPS adds a broader threat identification element to the analysis of each individual login.

The Adaptive Authentication module uses challenge questions as a means to confirm the identity of users. EPS employs strong user-selected queries based on personal non-public information. These challenge questions steer clear of data that would be generally available on the Internet or from other semi-public sources such as credit bureaus or online financial sites.[9]

ProfitStars also offers a token-based solution for the EPS Merchant Portal. This model requires users to enter a token-generated one-time password (OTP) during each login. This feature utilizes tokens from VeriSign®, an icon in the online security industry.

Financial institutions choose the multifactor authentication method that best suits the needs of each merchant. The flexibility to assign Adaptive Authentication or tokens on a business-by-business basis allows the FI to apply the appropriate level of security to each merchant based on the risks associated with that particular client.

IP Address Restrictions

Financial institutions may also work with each corporate client's IT team to create a "white list" of acceptable IP address ranges. When this security measure is implemented, users from non-approved IP addresses will be prevented from entering the system. This security measure helps prevent account takeover by blocking illicit users, even if they have stolen valid credentials from legitimate users. It may also prevent session manipulation attacks launched from servers outside of the allowed range of IP addresses.

News Posts

When a user logs in to the system, he or she may view optional "news posts" made available to them by their financial institution. While news posts may not be widely viewed as a security tool, they do give FIs the ability to post security reminders to their customers or members, warn users about specific fraud types that may be occurring more frequently, and make users aware of system changes or additional new security features.

Transaction Submission Security Measures

Strong user authentication alone cannot prevent fraud. In trusted entity theft, legitimate users create fraudulent transactions after they are authenticated. Account takeover artists evolve and continue to find ways to thwart each new authentication method. Session manipulation attacks are designed to compromise online sessions after legitimate users have been authenticated.

For these reasons, a second layer of security measures must be embedded in the part of the transaction process where funds transfer requests are initiated. This security layer provides additional protections that help prevent the creation and/or fulfillment of fraudulent transactions.

EPS provides a variety of transaction controls that help prevent fraud. When combined with strong user authentication measures, these transaction-related checks form a more effective barrier against the illicit movement of funds.

[8] While the most recent FFIEC guidance questions the effectiveness of simple device identification, it confirms support for complex device identification. (See the "Device Identification" section on page 6 of the guidance for more information.) In its *Solutions to Address the FFIEC Guidance* white paper, RSA confirms that its solution uses complex device identification: "RSA Adaptive Authentication leverages the RSA Risk Engine which performs complex device identification to meet the requirements of the FFIEC Guidance. The device identification process looks at a diverse set of data to establish the authenticity of a device including tracking device characteristics that are a natural part of any device (HTTP headers, operating system version, browser version, languages, and time zone), the IP address and enriching it by extracting IP geo-location details and additional information such as the ISP, IP owner, and connection type, and actively introducing additional identifiers through the use of a cookie and/or a flash shared object (also referred to as "flash cookie") which serve as more unique identifiers of the device." (See http://venezuela.emc.com/collateral/solution-overview/11502-ffiec-sb.pdf.)

[9] In its most recent guidance, the FFIEC recommends "out-of-wallet" challenge questions based on information obtained from external sources such as credit bureaus. (See the "Challenge Questions" section on page 6 of the guidance for more information.) While ProfitStars plans to utilize such questions to help confirm the identity of consumer users, we feel the use of such methods to confirm the identity of commercial users is inadvisable. Acquiring data to produce this type of out-of-wallet question would require storage of detailed personal information (such as home address, date of birth, Social Security Number, etc.) for commercial users. The entry and maintenance of this data creates its own security risks. ProfitStars believes that the extremely personal nature of the challenge questions embedded in its applications meets or exceeds the out-of-wallet requirement while avoiding the risk of storing detailed personal information for commercial users.

Velocity Controls

The EPS Merchant Portal provides unsurpassed velocity controls for online payments, allowing financial institutions to set thresholds by merchant, location, transaction type, or settlement type, and by template group for mobile consumer RDC. These limits help FIs identify scenarios where fraudsters attempt to move large sums of money in a short period of time. These thresholds increase the likelihood that fraud attempts will be discovered before losses become excessive.

In addition to single transaction and single-day calculations, velocity controls are also applied to a rolling 14-day period to further insure that user activity is within expected norms. Velocity controls include the following threshold elements:

- Single transaction amount.
- Daily transaction count.
- Daily transaction amount.
- Period transaction count.
- Period transaction amount.

These threshold elements can also be established separately for each ACH SEC code as a means to further tailor velocity controls to match specific types of payment activity.

The Merchant Portal displays configurable warning messages based on how near the client is to exceeding their thresholds. Financial institutions may suspend, decline, or accept velocity exceptions once they have researched the event and assessed the risk of processing the transactions.

Dual Control

Financial institutions and/or merchants may, on a user-by-user basis, enforce dual control for keyed ACH transactions as well as checks scanned using Merchant Capture (Scan Check) in the Merchant Portal. When enforced, this security measure will require a second user to review and approve submitted transactions.

In the Merchant Portal, dual control requirements can be invoked based on threshold amounts. The authority to process transactions can be limited for each user. This capability allows financial institutions and/or merchants to create scenarios where small transactions may pass through the system quickly while larger transactions would require approval from any one of a pool of users, and even larger transactions may require the approval of a handful of designated executives.

Dual control is a powerful measure that will help mitigate trusted entity theft and account takeover attacks. Dual control also helps prevent fulfillment of fraudulent transactions generated in a parallel session as part of a man-in-the-middle attack.

Duplicate Item Detection

The EPS Merchant Portal identifies and blocks submission of previously deposited checks. As items are deposited, they are compared against the previous 75 days of transaction history. When duplicate items are detected, those items are rejected. Users may view a report listing duplicate items, complete with a link to the original transaction's detail information to help identify why the current transaction is considered a duplicate.

Because duplicate detection is performed by the EPS processing engine, duplicates can be detected even when items are "deposited" by the same client through different sources. If, for instance, a merchant scanned a check but also presented that same check through an alternate source that submits items through the Web Services API or via file upload, the EPS engine would likely identify the second instance of the item and designate it as a duplicate.

EPS Keying and Balancing Service

The EPS Merchant Portal offers a unique security service for remote deposit transactions. Financial institutions that use the EPS keying and balancing service are better able to protect themselves against erroneous – or fraudulent – data entry during remote capture.

While some systems allow the merchant to edit items manually, the EPS Merchant Portal can prevent merchant users from making changes to remotely deposited checks. Instead, ProfitStars EPS representatives review exception items and balance deposits on the financial institution's behalf. Implementing this service helps mitigate trusted entity theft perpetrated through malicious editing of remote capture items.

FI Review and Processing Security Measures

Combining effective user authentication and strong transaction controls should prevent many types of fraud. Even so, these measures are not enough. Financial institutions must also establish a final security layer that includes thorough review mechanisms and processing controls in order to identify anomalous user activity and examine suspect transactions.

EPS incorporates industry-leading analysis tools that give financial institutions the ability to review system activity intelligently. In addition, planned enhancements will provide powerful new state-of-the-art fraud identification and research capabilities.

On-Demand Reporting

The EPS transaction processing engine sports one of the industry's most robust report generation modules. This reporting tool allows FIs to perform criteria-driven searches of historical payment data across all current clients and transaction types. The reporting engine also provides on-demand security reports detailing login failures and IP address violations, as well as sophisticated velocity reports that help FIs monitor and resolve velocity exceptions.

This reporting tool dramatically improves a financial institution's ability to research suspect transactions or to perform a detailed analysis of a company's activity.

Actionable Data Analysis with SmartSight™

SmartSight is an unparalleled interactive dashboard that provides actionable insights and gives financial institutions the ability to monitor and analyze historical and real-time customer data for reporting, strategic business, and risk mitigation purposes. This innovative solution provides financial institution executives and senior operations staff with a convenient tool for viewing and analyzing remote deposit, ACH, and card transaction data within the EPS platform.

SmartSight effectively displays consolidated information with an easy-to-use, graphical interface that helps measure, monitor, and analyze risk and customer activity. Users can gain global insight into trends in key performance indicators for specific businesses or FI-defined segments. Detailed information is also available through SmartSight's interactive drill-down capabilities.

In its current-day dashboard, SmartSight displays up-to-the-minute data about transactions as they are being processed. From this dashboard, users can drill down to view processing information for businesses, individual transactions, or scanned images. Users can even approve or void transactions from within the SmartSight user interface.

Some of the key features of SmartSight include:

- Graphical charts and displays with drill-down functionality.
- The ability to display and drill down into transaction activity by a variety of criteria, such as payment type, SEC code, amount, and count.
- The ability to export data to Microsoft® Excel®.
- The option to create FI-defined business segment groupings.
- Real-time transaction monitoring, including the ability to search, approve, or void transactions.
- Return transaction monitoring, including return reason detail.
- The ability to analyze risk limits, thresholds, and tolerance levels at the business or location level.
- The ability to review velocity limits, utilization, and trending.

SmartSight assists FIs in meeting examiner expectations by helping them measure and monitor risk across multiple payments channels (ACH, checks, and card transactions). The 2009 FFIEC guidance entitled *Risk Management of Remote Deposit Capture* requires institutions to monitor risk from both a point-in-time perspective as well as trends over time.[10] SmartSight helps address these regulatory requirements with graphs indicating both point-in-time status and temporal direction.

This solution uniquely provides FIs the ability to compare "like-business" transactions and activity quickly. Return transactions and exceptions are easy to track. SmartSight clearly displays exposure limit utilization, which is a key metric for evaluating and mitigating risk.

System Administration Security Measures

An appropriately deployed security system with layered solutions spread across the user login, transaction submission, and FI review phases should help mitigate fraud attacks directed at the business user side of online payment applications. However, financial institutions must also be diligent in policing administrative access to the system.

The most recent FFIEC guidance affirms this requirement as one of the specific elements for future examinations.

EPS provides a variety of strong administrative controls to help prevent "back-door" fraud. Planned enhancements will add additional measures to further strengthen this vital area.

Multifactor Authentication

Financial institution users may utilize the same token solutions in the Partner Portal that were identified in the "Multifactor Authentication" subsection of the "User Login Security Measures" section above.

Dual Control for Profile Changes

EPS allows FIs to implement dual control when new capabilities are added to user profiles in the Merchant Portal. When enforced, changes to user profiles will not take effect until they are reviewed and approved by a second administrator.

This feature is a key security measure to assist in protecting against account takeover at the corporate or financial institution level. It helps prevent fraudsters who gain access to an administrator's credentials from establishing new users with which they could circumvent the system's dual control measures.

EPS SmartPay Express™, Customer Payment Portal™, and Hosted Pay Page™ Security Measures

SmartPay Express (SPE), the Customer Payment Portal (CPP), and the Hosted Pay Page (HPP) are optional business-branded, ProfitStars-hosted websites that funnel consumer-initiated payments into the EPS transaction processing engine. These modules are used by corporate clients or non-profit organizations to collect payments or donations made by consumers.

The 2011 FFIEC guidance considers consumer transactions generally less risky than commercial transactions.[11] Because CPP and HPP are consumer-facing, they use different types of user access controls than the Merchant Portal's corporate payment modules. However, since CPP and HPP payments flow into the main EPS processing engine, the review and processing functions for CPP and HPP payments are virtually identical to the review and processing functions for remote deposit, ACH, and card payments collected through the Merchant Portal.

Accordingly, financial institutions may assume that security measures mentioned in these sections do not apply to SPE, CPP, or HPP:

- User Login Security Measures
- Transaction Submission Security Measures

[10] *Risk Management of Remote Deposit Capture*, FFIEC, January 2009, p.8, final paragraph.

[11] *Supplement to Authentication in an Internet Banking Environment*, June 2011, p. 3, final paragraph.

In contrast, security measures mentioned in these sections do apply to these products:

- FI Review and Processing Security Measures
- System Administration Security Measures

Implementing New Security Controls

In response to FFIEC requirements, financial institutions may find it necessary to amplify existing online payment system security measures and append new ones. It is critical that FIs spend the time and resources to perform thoughtful, thorough risk assessments. An accurate analysis of current and future threats is essential if financial institutions are to make the right choices about security changes.

Before deploying new security measures, financial institutions should also consider the impact of the changes on corporate users' daily processing activities. It will be crucial for banks and credit unions to communicate these changes to their clients in advance. New security measures will be most effective when financial institutions implement them in partnership with their customers/members.

Other Resources

ProfitStars is committed to supporting its financial institution clients as they continue the ongoing effort to meet the requirements of a changing security landscape. This partnership is the surest way for both vendors and financial institutions to secure their online payment systems.

ProfitStars' Support teams are available to assist financial institutions with online payment security questions. Our representatives can discuss security features or help guide institutions through configuration changes. Our Support teams can also connect financial institution staff members with EPS industry experts who can discuss broader security issues.

ProfitStars' Education group offers a wide range of education options, including onsite training, webinars, and recorded training sessions. Many of these sessions are dedicated to security topics. Financial institutions may wish to avail themselves of these resources as part of their ongoing effort to stay abreast of changes in the security landscape.

The resources below may also provide financial institutions with additional information to help them formulate their response to the recent FFIEC guidance.

- *Authentication in an Internet Banking Environment* (August 2001)
  http://www.ffiec.gov/pdf/pr080801.pdf
- *Authentication in an Internet Banking Environment* – Update (October 2005)
  http://www.ffiec.gov/pdf/authentication_guidance.pdf
- *Risk Management of Remote Deposit Capture* (January 2009)
  http://www.ffiec.gov/pdf/pr011409_rdc_guidance.pdf
- *Supplement to Authentication in an Internet Banking Environment* (June 2011)
  http://www.ffiec.gov/pdf/auth-its-final%206-22-11%20(ffiec%20formated).pdf
- FFIEC IT Examination Handbook Infobase
  http://ithandbook.ffiec.gov/it-booklets/information-security/introduction/regulatory-guidance,-resources,-and-standards.aspx
- FDIC Technology Regulations and Publications for Financial Institutions
  https://www.fdic.gov/regulations/resources/director/risk.html
- NACHA Corporate Account Takeover Resource Center
  http://www.nacha.org/corporate_account_takeover_resource_center
- NACHA Operating Rules Updates and Upcoming Changes
  https://www.nacha.org/rules/updates
- NACHA Risk Updates and Resources
  https://www.nacha.org/risk
- ProfitStars FFIEC Authentication Guidance Knowledge Center
  http://discover.profitstars.com/home-noncore-0/

About ProfitStars

Information in this document is subject to change without notice.

This white paper is provided by Jack Henry & Associates solely as a convenience to its ProfitStars Enterprise Payment Solutions customers and is not intended to serve as a substitute for FFIEC guidance documents or provide legal advice or interpretation regarding the requirements of the NACHA Rules, the examination requirements of the FFIEC, or any other legal aspects of processing ACH transactions. The reader of this white paper should become familiar with the provisions and requirements of the FFIEC and should seek competent business and legal advice from his or her organization's legal counsel and compliance officer, and exercise his or her own judgment in applying appropriate security measures. While Jack Henry & Associates has exercised care in accurately summarizing the contents of selected FFIEC guidance documents in this white paper, it cannot guarantee that its summary of those guidance documents provides a comprehensive treatment of the laws or regulations applicable to ACH processing or that this white paper is completely up to date with the latest guidance that may be issued by the FFIEC from time to time. The FFIEC has not reviewed or endorsed the analysis or conclusions contained in this white paper.