Security Controls and Best Practices for Financial Institutions

By Robert Lee
Senior Security Product Manager
December 2010
I. Overview ............................................................................................................................................. 3
II. The Threat Landscape and Compliance .............................................................................................. 4
III. Combating Compromised Credentials .............................................................................................. 5
    A. Password Security ...................................................................................................................... 5
    B. Enhanced MFA (EMFA) ........................................................................................................... 6
    C. Hardware Tokens (Business/Commercial Banking Only) ......................................................... 6
IV. Combating Local Malicious Software and Phishing ........................................................................... 7
    A. Trusteer’s Browser Security ........................................................................................................ 7
    B. VeriSign Extended Validation Certificates ................................................................................ 7
    C. RSA Fraud Shutdown ................................................................................................................ 7
    D. Separation of Duty, Positive Pay, & Limits (Business/Commercial Banking Only) ............. 7
    E. Limits ............................................................................................................................................. 7
V. Alerting (Business Banking and Business Financial Services only) ..................................................... 8
VI. Training & Best Practices ................................................................................................................. 8
VII. Action Plan ..................................................................................................................................... 10
VIII. Glossary ......................................................................................................................................... 11
      Guidance Materials ....................................................................................................................... 14
      Additional Resources ..................................................................................................................... 14
Overview

Recently the industry has seen increased sophistication of the technology used to commit fraud. There has also been a rise in the number of fraud incidents and average losses per incident. According to the Internet Crime Complaint Center (IC3), losses more than doubled between 2008 and 2009.

The intent of this document is to inform Financial Institutions about the online fraud threats they currently face. For each threat we discuss, we will provide some basic guidance about an available control that could mitigate the threat. This guidance represents a starting point for improving security.

Intuit strongly recommends that you review your current security plans and policies, make any updates necessary, and communicate improvements to your customers or members. For more information about helping users, visit the security page of the Intuit Financial Services Client Site at https://www.diclentsite.com/security/index.html.

* Source - Internet Crime Complaint Center

This document provides an overview of threats Financial Institutions face, and some basic controls. This document is not a substitute for the advice of regulatory advisors.
In order to commit online fraud, a fraudster simply needs to authenticate as the victim, using that victim’s online credentials.

For environments that rely on Single Factor Authentication (something the user knows), the fraudster can coax this information from a real user through compelling phishing campaigns, key logging, or Man-in-the-Middle proxy attacks.

For environments that have deployed Two Factor Authentication (something the user knows, and something the user has), fraudsters are now using enhanced malware installed on the victim’s system. This enhanced malware can stay dormant until the real user has completed the Two Factor Authentication, and then simply hijack the authenticated session. Once the session has been hijacked, the fraudster has the same access as the real user, allowing them to change contact information, change passwords, create new payees, and initiate funds transfers.

Financial Institutions have worked hard to create a trusted relationship with their customers. Users assume their Financial Institution is providing a safe online banking solution. Failure to meet this expectation will result in both hard losses in the form of fraud, but also a damaged relationship with the customer, and potential damaged brand reputation for the Financial Institution. While there is no single solution to combat every threat, Intuit has documented the most common threats that lead to fraud, and offers effective mitigation controls for each identified threat.

To combat these threats, we all have a role to play. Financial Institutions need to update their security controls as outlined in this document, and educate their end users about how to implement these controls. The end users of the online banking systems should put into practice the recommendations communicated to them by their Financial Institution. As the threat landscape evolves, so too must the controls that mitigate the risks.

A. Compliance

In late 2006, the Federal Financial Institutions Examination Council (FFIEC) published a handbook outlining security recommendations and best practices. This provided the first direction by the U.S. government in defining reasonable security standards with which Financial Institutions were required to comply. The FFIEC also instructed regulators and examiners to include these measurements when determining the passing status of the bank or credit union examination.

We expect the FFIEC to update their guidance regarding authentication and other security controls sometime in 2011.

Financial Institutions must also address the Uniform Commercial Code, Article 4A, which addresses fraud transfers, other than consumer transactions governed by the Electronic Fund Transfer Act of 1978. Though article 4A is written from the standpoint of the Financial Institutions and gives them a “safe harbor” from losses associated with wire, ACH, or other fraud, Financial Institutions are required to meet three conditions: (i) The bank and its customer agree to use a particular procedure for verifying the authenticity of wire transfer orders, (ii) The bank must provide a “commercially reasonable method of providing security against unauthorized payment orders” to the customer, and (iii) The bank followed the procedures in good faith compliance with agreement and instructions of the customer. This last statement refers to the security tools, policies and procedures of the bank, in short, the security controls and best practices.
Intuit has two primary goals for security: establish that the end-user authenticating is correct, and determine the online operations we process are what the user intended. If we accomplish these two goals, the rest of the online banking experience is as expected. Authentication is the process we use to determine if we have the correct user, or to validate if the operation was intended.

User credentials uniquely identify each person who uses the banking platform. The intent of authentication is unequivocal verification of the user’s claimed identity.

There are three main factors used for authentication:

- **Something the user knows (passwords)**
- **Something the user has (physical token)**
- **Something the user is (biometrics).**

When an authentication system uses more than one factor of authentication, the system has a higher assurance that the user authenticating is the correct and intended user of the account. Due to the highly sensitive nature of financial transactions, Intuit provides Multi-Factor Authentication.

Authentication can also be required “in-session”, or after login, as part of the handling of a transaction. This is used frequently as part of a wire transaction approval and some ACH transactions. In the future, other electronic fund transfers (EFT) and access to sensitive user configurations may also use additional authentication beyond the initial login requirements.

**A. Password Security**

A password represents a shared secret, known only by the end-user and the system they are authenticating against. The system cannot differentiate the real user from another user who also knows the password. For this reason it is essential that users keep their password private and immediately report any suspected security violations.

A well chosen password has two important characteristics; it should be easy to remember, and hard to guess. Users should be advised not to write down the password anywhere.

Passwords should be changed on a periodic basis to counter the possibility of undetected password compromise. Passwords should be changed often enough so that there is an acceptably low probability of compromise during a password’s lifetime. To protect against undetected password compromise, the maximum lifetime of a password be no greater than 120 days.

Below is a list of some common password choices to avoid:

- Customer name, or family member, or pet’s name
- Social Security, Account, or Phone numbers
- Any part of your physical address
- Anybody’s birth date
- Other information that is easily obtained about the user
- Any username on the computer in any form
- A word in the English or foreign dictionary
- A password used on another site
- Any of the above spelled backwards
- Out of Wallet or Public Records (e.g. Mother’s maiden name)
- Sequences: “12345678,” “222222,” “abcdefg”
Below is an example of a more secure password:
*iwc8dc*

- at least 6 characters in length
- at least one numeric digit
- not based on word in the dictionary
- not easily guessed
- can be easily remembered by remembering the letters stand for “Integrity Without Compromise, the number 8, and Delight Customers”.

Below is an example of a less secure password:
*money1*

- is based on a word in the dictionary

**B. Enhanced MFA (EMFA)**

New enhancements have made Intuit’s Enhanced Multifactor Authentication (EMFA) more secure than ever. Intuit strongly recommends that Financial Institutions implement this new security enhancement as soon as possible. In addition, you should communicate the importance of these benefits to your customers or members.

With EMFA, after successfully authenticating with their Username and Password (*something they know*), a One-Time Password (OTP) is sent to the user’s phone (*something they have*). The user must then enter this OTP into the banking application to complete the login.

The user may receive this OTP via a voice call or text message. EMFA provides a secure, low-cost and easy-to-use second factor of authentication. EMFA reduces the risk of credential exposure due to phishing, keystroke loggers, Man in the Middle, and brute force attacks.

The Enhanced MFA solution conforms to the latest FFIEC authentication requirements. If you require MFA as part of your FFIEC compliance, you must deploy the Enhanced MFA (Out-of-band OTP, or Token OTP) solution.

**C. Hardware Tokens (Business/Commercial Banking Only)**

As discussed in the Threat Landscape and Compliance section of this document, the newest fraud malware is capable of hijacking sessions and initiating funds transfers. The Business Banking and Business Financial Services platforms can require an additional OTP authentication challenge for each Electronic Funds Transfer (EFT) attempt.
A. Trustee’s Browser Security

Man-in-the-Browser (MitB) malware allows a fraudster to not only steal passwords and user IDs, but also modify the communication between the browser and the banking application. The malware can rewrite the account and payment instructions (such as the payee and amount), without the user’s knowledge, in real time.

Fraudsters have been targeting small businesses, as they typically have fewer security controls, yet still have enough money in the account to be attractive ($100,000 or more).

Intuit’s partnership with Trusteer provides an end-user system security control to combat MitB. Trusteer’s Rapport, is an anti-malware solution that isolates the browser process from other processes on the system. In addition, Rapport provides a violation report and alert feature that informs your institution of logged Trojan attempts so you can monitor your user base infection rate.

Rapport is a critical security control used by many leading Financial Institutions that can reduce the risk of losses from MitB based attacks. This offering is strongly recommended for all customers given the nature of the attacks, but it is particularly crucial for users with Wire and ACH transaction features.

B. VeriSign Extended Validation Certificates

Intuit offers the highest level of extended validation certificates, Secure Site Pro with Extended Validation SSL Certificates by VeriSign. These certificates provide a 128-bit encrypted connection between the user’s browser and the web services. Extended Validation (EV) Certificates provide visual indicators, including a green address bar and padlock at the header of the browser, as well as a VeriSign seal at the footer of the website to give confidence to users that they are at the correct website. User training for EV Certificates is available online at the site: https://www.phish-no-phish.com

C. RSA Fraud Shutdown

RSA’s Fraud Shutdown Service proactively monitors the web for your brand. In the event that your organization is subject to a phishing attack, RSA will work with ISP’s and law enforcement to shutdown the servers hosting the phishing site. Both the VeriSign EV certificates and RSA’s fraud shutdown are essential controls against phishing attacks, which have become more dangerous over the last year.

D. Separation of Duty, Positive Pay, & Limits (Business/Commercial Banking Only)

The Separation of Duty control is available for ACH and Wire transactions. With separation of duty, one user has permission to initiate a funds transfer, while a secondary user must approve the transfer. By separating the capabilities in this way, you prevent a scenario where a single user could transfer funds independently without oversight, or where a fraudster could move funds with a single set of user credentials. This would require a fraudster to gain control of both account types to successfully transfer funds. This method can even be effective against the MitB malware as the approver will have the fraudulent payee and amounts revealed to them before the transaction is finalized. The approver can detect the fraudulent amounts or payees and prevent the attack or inform their organization before the loss occurs. If used, this control can be an effective method of reducing the fraud risk and ensuring customer involvement and awareness.

E. Limits

Organizations should establish limits that restrict the dollar amounts allowed for a Wire or ACH transaction. Creating such dollar limits can reveal attempts to violate those limits and reduce single loss expectancies for your customers. Limits may be established at the customer, user, or transaction level. Because this is a business decision as well as a risk matter, you must decide what level of transaction risks you are willing to take. A recommended approach to this is to monitor the customer’s transaction behavior and determine what is suitable.
Alerting (Business Banking and Business Financial Services only)

Activity Reporting - On-going data and statistics on the state of online activity is another important best practice for security. Your institution should be encouraging customer administrators to run activity reporting on a daily basis and to scan for logins from unidentified IP addresses during off-hours.

The goal is to identify any suspicious or abnormal activities. We recommend that you communicate and encourage your members to take such actions, as activity reports will provide records in the event of a fraud investigation. For your part, you can provide customers with balance alerts via email.

Training & Best Practices

The changing mindset of consumers and businesses toward their safety while online makes the role of education essential. Your trusted relationship depends on the strength of customer confidence in your online site and goes beyond the online experience. Intuit can provide you with Privacy and Protection materials you can post on your website. These materials were designed to provide your users with clear, understandable security best practices. Moreover, we encourage you to engage your customers and members with security guidance whenever possible. Some of the approaches include:

1) Online discussion forums and social networking sites for your Financial Institution
2) Alerts and notifications on key security tips
3) Quick tips for the Financial Institution’s customer service teams to pass along during a support interaction
4) Community roundtables and talks whereby you can provide end-user best practices, such as those noted in the Password Security section of this document and the Privacy and Protect materials
5) Include dedicated sections for security feedback in your message boards to allow customers a voice

Recent research has shown that as many as 82 percent of online users expect to participate in security.1 This is an opportunity to make security part of your trusted brand and to involve users in the process. Additionally, well informed users can aid in their adoption and support of your security controls and policies.

Your institution should establish written policies for Wire/ACH Sales manager training that emphasizes security, customer awareness and the importance of security controls. You should also require written disclosure and acknowledgement by an officer or owner of the business that they have read, understand and agree to implement all security practices. Commercial clients should be informed of best practices for them and how you can help via your security offerings as well as policies they can employ to protect themselves. The following is a list of best practices for your commercial clients, which can act as a guideline for your recommendations to them:

- Monitor accounts frequently (daily as a best practice). Immediately review Wire, ACH or other transaction confirmations.
- Implement dual controls and approval for ACH and Wire transfers so that dual approval is required before the transaction is initiated at the Originating Depository Financial Institution (ODFI).
VI. Training & Best Practices (continued)

- Never share user IDs, passwords, PIN numbers, dynamic tokens, etc. with anyone. Do not leave them in an area that is not locked/secured.
- Do not use the same login or password on any other website or software.
- Obtain and install antivirus, anti-malware and anti-spyware software, and consider installation of a firewall (and make sure it is active and automatically updated by the vendor, or take necessary steps to keep it updated).
- Limit or eliminate unnecessary web-surfing and/or e-mail activity by employees, including personal activity, on computers used for online banking.
- Consider a dedicated computer for online banking that is never used for e-mail or general internet browsing/surfing (cost of computer vs. loss).
- Educate all company/entity personnel on good cyber security practices, clearing the Internet browser’s cache before and after visiting the Financial Institution’s website, to avoid having malware installed on a computer.
  » e.g., if a media player needs to be updated, go to the official media player website to install the update. Clicking on a fake update installation link could just mask a hacker downloading malware onto the computer.
- Verify use of a secure session. (“https://” and not “http://”)
- Avoid saving passwords to a computer.
- Never leave a computer unattended when using any online banking service, and always lock your computer when away.
- Never access the Financial Institution’s website for online banking (or any privileged or sensitive computer system) from a public computer at a hotel/motel, library, coffee house or other public wireless access point.
- Be suspicious of any employment position that requires use of a personal account for business purposes. Such offers for employment as a mystery shopper, payment processor, etc., where you are required to use your personal account for someone else’s business purposes, are not legitimate.
  » No legitimate business will attempt to move business funds through anyone’s personal account, and you should educate yourself on these issues.
  » If you are approached to participate in such schemes, immediately contact local law enforcement, the FBI or the Secret Service to let them know.
Now that you have reviewed various security controls and recommended best practices it is important to consider these controls as they relate to your risk assessment and specific business needs. Below is a summary of some security threats and controls.

- **Phishing:** Technique used by fraudsters to acquire username, password and other sensitive information through social engineering by masquerading as a legitimate website, message or other communication. Credentials are generally captured and sent to a command control service then used or resold for later use by criminals.
  - Enhanced Multifactor Authentication
  - VeriSign Secure Site Pro with Extended Validation SSL Certificates
  - RSA Online Fraud Shutdown

- **Password Compromise:** Attempts to ascertain passwords from data stored or communicated to your online services. Common approaches of guessing passwords are now done programmatically by sophisticated algorithms including dictionary attacks that experiment with common word usage.
  - Enhanced Multifactor Authentication
  - Password lockout and strict character and reset policy control
  - VIP/GoID Hardware Tokens (Wire and ACH only)

- **Crimeware Trojans:** Malicious code designed to steal funds by conducting fake Wire, ACH and other EFTs in real-time without the user’s knowledge. These Trojans lay dormant on the user’s machine until the user authenticates an online session, then the malicious software hijacks the authenticated session and attempts fraudulent money movement.
  - Trusteer’s Rapport Security Browser
  - Separation of Duty Controls (add VIP/GoID for more effectiveness)
  - ACH Positive Pay
  - Third Party Alerting

When planning your approach, make sure to include communication activities with information regarding all of the security techniques you choose to employ.

When planning your approach, make sure to include communication activities with information regarding all of the security techniques you choose to employ. This should be approached as part of an education and awareness effort, but should also disclose and inform users of your security policies, procedures and controls. Moreover, you must get written acknowledgement of users’ understanding and agreement of use.

In summary, the most effective control against fraud is a well informed user. The benefits to your organization are not just a reduction in risk, but also a foundation for a trusted relationship which not only defines their online experiences but goes beyond it.
Authentication Factors
There are three main factors used for authentication:

- Something the user knows (passwords)
- Something the user has (physical token)
- Something the user is (biometrics)

For an authentication solution to be considered multi-factor, it must have two or more different factors included. Supplementing the user-name + password with a challenge question is multi single-factor, not multi-factor.

Key Logging
Key loggers monitor what is being typed at keyboards, and what mouse movements or clicks are being generated. Key loggers come in hardware and software versions. A fraudster can go through the logs looking for account credentials and answers to challenge questions. Sophisticated software key loggers can also capture what is displayed on the screen.

Key logging is effective against sites that use single-factor authentication (username, password), or multi single-factor authentication (username, password, challenge questions).

Man-in-the-Browser (MitB)
Man-in-the-Browser (MitB) attacks move the proxy function of a Man-in-the-Middle (MitM) attack from an external application into an extension of the browser itself. In essence, MitB is a sophisticated variation of MitM.

In a MitB attack, the fraudster still has visibility into all data sent or received. Fraudsters can still collect login, password, and challenge question information. Additionally, fraudsters can use the already authenticated session to independently navigate the site, adding new payees or initiating funds transfers, without displaying any of their activity to the browser screen.

For sites that use Multi-Factor Authentication, the MitB can stay dormant until the user initiates an action the fraudster is interested in, such as adding a new payee. At the time the new payee is added, the MitB can alter the data being sent to the banking site, while still displaying what the user entered back to their browser screen.

For example, user adds account #12345 as a new payee. MitB alters what is sent to the banking site to account #31254. User is prompted for a One Time Password (OTP). User receives OTP via SMS. User enters OTP into browser to authenticate the payee addition. The confirmation page on the user’s screen shows payee #12345 successfully entered, while the banking application actually has a new payee of #31254.

MitB attacks are effective against sites that use single-factor authentication (username, password), multi single-factor authentication (username, password, challenge questions), and multi-factor authentication.

Man-in-the-Middle (MitM)
In a Man-in-the-Middle (MitM) attack, users believe they are interacting directly with a real banking site, when in reality there is a proxy function that is intercepting, manipulating, and forwarding the data between the user’s browser and the real banking site.

MitM attacks are effective against sites that use single-factor authentication (username, password), or multi single-factor authentication (username, password, challenge questions).
Multi-Factor Authentication
Multi-Factor Authentication enhances the authentication process by adding an additional factor to be validated. Generally accepted authentication factors include, something the user knows (shared secret), something the user has (physically in possession of), or something the user is (biometrics).

Typical multi-factor authentication in online applications pair something the user knows with something the user has. For example, many Financial Institutions issue a hardware token that generates a time bound One-Time-Password (OTP) as a secondary factor. If a fraudster knows the username and password for an account, but does not possess the hardware token, they are not able to authenticate.

Multi-Factor Authentication mitigates compromised user credentials, password reset attacks, phishing attacks, key logger attacks, and some MitM attacks.

Out-of-Band Communication
Out-of-Band (OOB) communication is messaging sent to a user in a separate channel than the web browser. OOB Communication provides a secure messaging channel separate from a potentially compromised desktop system.

Password Policy
The main components of a password policy involve the password space, the lifetime of a password, and the rate at which passwords can be guessed. All of these components are configurable by an FI administrator.

S: The password space is determined by the total number of characters in the password alphabet, and the length of the password. For example, a 6 digit, alpha-numeric password has a password space of $36^6$.

L: The lifetime of a password determines how frequently a user must change their password. For the example below, we will assume 120 days.

R: The rate at which an attacker can guess a password is controlled by how many consecutive failed logins are permitted before automatic account lock out. If we assume an auto lock out after 3 consecutive failed attempts, and further assume that the real user logs in on average once per day, we can assume a rate of 2 guesses per day.

P: The percentage of the password space that can be exercised (brute forced), given the password length, the alphabet size, the lifetime of the password, and the rate at which guesses can occur can be expressed as: $P = (L \times R) / S$

In the case of a 6 digit alpha-numeric password, with a 120 day lifetime, and a 3 failure auto account lock out, a brute force attempt will only get through 0.000011% of the password space.

Password Reset
On some sites, the password for a user can be reset if certain challenge questions are correctly answered. In many cases the answers to the challenge questions are easier to guess than the original password.

Online social sites (Facebook, Myspace, etc) allow users to send benign looking surveys, seemingly to help friends get to know each other better. Many of the questions in these surveys reveal the answers to some of the most common challenge questions used by online sites.
**Phishing**
In a phishing attack, fraudsters create a website that impersonates a real banking site. The fraudsters lure users to this impersonation site where the user will try to authenticate. Once credential information is entered, the fraudster can use this information to log into the real banking site.

Phishing is effective against sites that use single-factor authentication (username, password), or multi single-factor authentication (username, password, challenge questions).

**Single-Factor Authentication**
Most applications support single-factor authentication; something the end user knows (username and password). Many banking applications require a set of challenge questions to enroll a new system. Since a challenge question is also answered by something that the user knows, it is not a second factor. The application keeps track of which sessions have been authenticated.

Once a fraudster has this data, they can log into the account from any system on the internet. There is typically no additional authentication required to add new payees or to initiate a funds transfer.
Guidance Materials
- E-banking Booklet (August 2003)
- FFIEC Authentication (OCC 2005-35)
- Information Security Booklet (July 2006)
- ACH Risk Management (OCC 2006-39)
- FFIEC IT Examination Handbook (February 2010 – updates)
- Consumer Compliance
- BSA/AML
- ID Theft Red Flags (FACTA)

Additional Resources
- NACHA ACH Operations Bulletin: “Corporate Account Takeovers Can Lead to Fraudulent Transactions” (12/2/09)
- For more information about helping users, visit the security page of the Intuit Financial Services Client Site at https://www.diclientsite.com/security/index.html