Template

Purpose

- This is a "template" Customer Awareness Training Strategy to be used as a "starting point" for the sake of helping you develop your own Customer Awareness Program.

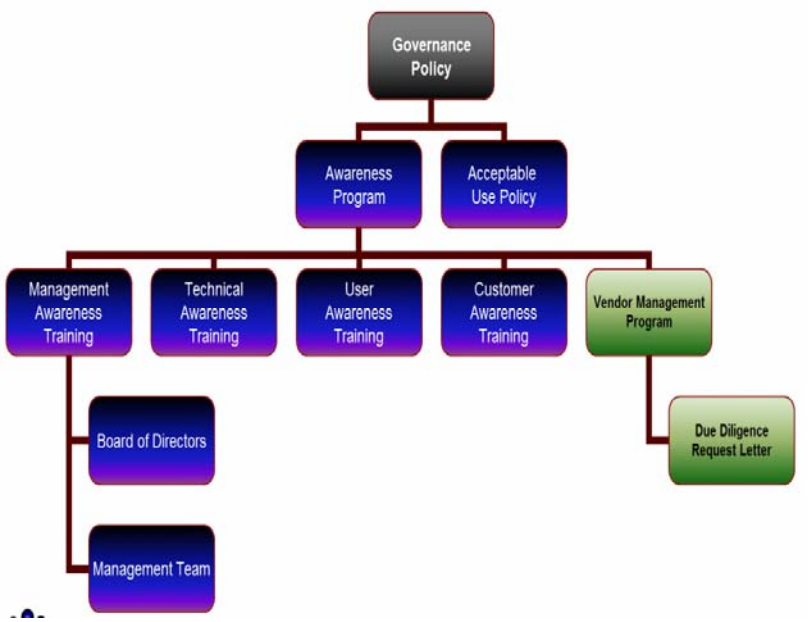
Copyright / Permission to Use

- Permission to use this document is conditional upon you receiving this template directly from an **infotex** employee, **infotex** website or e-commerce site, or an **infotex** workshop / training presentation.
- By using this template either in its entirety or any portion thereof, you acknowledge that you agree to the terms of use as dictated in the "Transfer of Copyright Agreement" located at copyright.**infotex**.com. This agreement establishes that when you customize this template to your specific needs, your organization may have copyright of the customized document. However, **infotex** retains copyright to the template. This agreement also establishes that you will not share this or any other template with third parties other than auditors and examiners. You may not transfer ownership of the customized documents to any other organization without the express written permission of **infotex**.

Instructions

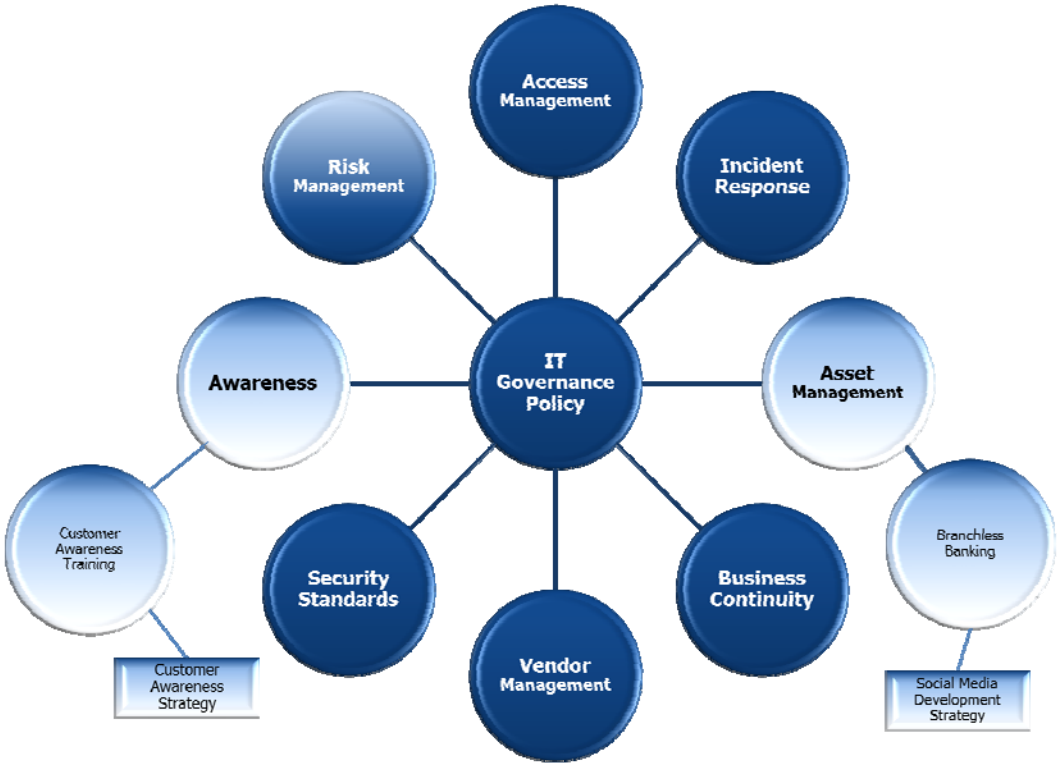
- Make sure to read through the template carefully as not all situations will pertain to your organization. However, to assist you in customizing the document to your specific needs, we have attempted to color code areas that will need your special attention. Color coding is as follows:
    - All areas needing customization and/or consideration are in **red**.
    - Sections that are in **brown** are optional sections according to our definition of best practices. These sections may be removed if they do not match your needs.
    - Sections in **blue** are merely instructions or additional information for knowledge purposes and should be removed.
    - Sections in **green** are examples.
- This section (Templates) may be removed once the document has been customized, for at that time we turn ownership of the customized document over to you.

NOTES ABOUT THIS BOILERPLATE:



- This document is intended to be part of the "customer" subprogram of the Awareness Training Program.
- This document gives birth to a "Customer Awareness Training Strategy" and other documents that are also part of the Awareness Training Program.

- The Customer Awareness Training strategy, though part of the Awareness Program, also has direct impact upon the Branchless Banking subprogram of the Asset Management Program, as well as the Social Media Strategy.



Iterations:

Iteration #: 4
Date of This Iteration: 06/06/2013
Original Iteration: September 2009

Next Update Due: 11/19/2014

Insert Financial Institution Name / Logo

Customer Awareness Training Strategy

(Approved During xx/yy/zz [IT Steering / EDP / Technology] Committee Meeting)

Classified: Internal Use

Contact if found: Name, Title
Name of Financial Institution
City, State

Strategy Scope

Consider the first paragraph carefully. You may want to escalate a definition of standards in your IT Governance Policy. Your Compliance Officer should approve of statements like this, just so that he/she can be aware that they exist. San-serif text is on purpose, but you can also change the text to match the normal text.

> "Note: This document is a strategy document, and thus is a collection of our current thoughts, guidelines, and potential plans. It is created with the knowledge that it therefore does not need to be submitted as part of an audit or examination production unless specifically requested. It is NOT a part of the formal IT Governance Program. It is merely documentation of our existing thoughts, guidelines, and potential plans on how to enforce particular policies and procedures. We do not, by documenting these thoughts and ideas, commit to enforcing them."

Or, if you'd rather be more informal about this, you could choose to not include the above section and instead include the following:

> "Note: The following strategies are meant for the [IT Manager / CIO / EDP Committee / etc.] and the [Information Security Officer] for training purposes only. These are unofficial standards, and this document is intended as a guideline, not a policy or procedure to be enforced. As such, it is an internal document and is not intended for review by examiners and/or auditors, unless, of course, this document is specifically requested."

Or, you could simply choose to not use either of the above two statements.

This strategy applies to all Name of Financial Institution's management team members and employees who come into frequent contact and communication with the institution's customers. The Information Security Officer is responsible for overseeing the development, implementation, and maintenance of this strategy. It should be reviewed at least annually to ensure relevant information is appropriately considered. For questions concerning this strategy, see the Information Security Officer.

Objective

Though we cannot always control the behavior of our customers, the efforts we make to influence good security practices will in themselves lower the impact of an information security or fraud incident. Management must recognize that customer awareness touches upon most areas of governance, including access management, incident response, asset management, business continuity, risk management, and vendor management. The training materials we provide our customers, the interactions between our front-line employees and our customers, and the manner in which disclosures, tips, guidelines, and policies are conveyed to our customers can increase or reduce risk, depending upon our approach.

Customer awareness training as a business function in any organization has always been an important component of an overall awareness training program. However, now that the June 2011 Supplement to Authentication in an Internet Banking Environment requires financial institutions to provide customer awareness training, it is important that we create a documented strategy that incorporates training for all types of customers.

The purpose of this strategy is to ensure compliance with the IT Governance Policy as it relates to awareness training for all four corners of the organization, as well as to ensure compliance with various laws and regulations that require specific disclosures or customer training.

Primary Strategy of Customer Education

Above all, we want our customers to adopt, over time, safe habits and disciplines in the way they use technology and information. Habits and disciplines are hard to instill, but the effort to instill them provides a great deal of value to the institution.

Top Priorities of Customer Awareness Training Strategy

1. Educate, Motivate, and Activate Customer Awareness of safe habits and disciplines.
2. Motivate Customers to Learn on their Own
3. Meet all compliance objectives established by the FFIEC and other regulations and regulators.
4. Establish legal risk mitigation practices.

Requirements of the June 2011 Supplement to the 2005 Authentication Guidance

According to the Federal Financial Institutions Examination Council's (FFIEC), a financial institution's customer awareness and educational efforts should address both retail and commercial account holders and, at a minimum, include the following elements:

- An explanation of protections provided, and not provided, to account holders relative to electronic funds transfers under Regulation E, and a related explanation of the applicability of Regulation E to the types of accounts with Internet access;
- An explanation of under what, if any, circumstances and through what means the institution may contact a customer on an unsolicited basis and request the customer's provision of electronic banking credentials;
- A suggestion that commercial online banking customers perform a related risk assessment and controls evaluation periodically;
- A listing of alternative risk control mechanisms that customers may consider implementing to mitigate their own risk, or alternatively, a listing of available resources where such information can be found; and,
- A listing of institutional contacts for customers' discretionary use in the event they notice suspicious account activity or experience customer information security-related events.

Opt-out and Hold Harmless

Note: consider the compliance and risk escalation implications of the next paragraph: The Financial Institution has, until regulatory enforcement is clarified, empowered management to offer certain controls as optional controls to certain customers. For example, at the time of this procedure's review, we require OOBA for our high-risk commercial customers, but make it optional for retail customers. The tactic for implementing this sort of waiver must be to accompany the waiver process with opt-out documentation. In other words, customers will be required (whenever possible) to sign an agreement

that expresses their understanding of the risks of opting out, that the institution has tried to educate them on the risks of opting out, and that they will hold the institution harmless for any losses that result from opting out of the control in question.

Note: If the above is adopted as strategy, the Information Security Officer should consider escalating the associated compliance risk to the board of directors.

Authority

The Information Security Officer will work closely with marketing personnel and web developers to ensure an adequate mix of identity theft prevention education is distributed to customers in the form of flyers, web page elements, and public announcements. In order to comply with the June 2011 Supplement to the FFIEC's 2005 Authentication Guidance, the Information Security Officer will maintain a Customer Awareness Training Strategy that will be updated annually.

The Customer Risk Assessment

Given that different types of customers present different levels of risk, and thus awareness training efforts should vary depending upon this risk, our strategy will start with an annual customer risk assessment. The customer risk assessment, like any other risk assessment, should start with an inventory. There are many perspectives with which we can view and thus categorize customers. The following represents a basic inventory of customers in a financial institution based on the type of business a customer conducts:

- High Risk Commercial Customers
- Moderate Risk Commercial Customers
- High Risk Consumers
- Moderate Risk Consumers
- Low Risk Consumers

This viewpoint works well given that regulations, specifically Regulation E which governs electronic funds transfers, differ for consumer and commercial accounts. Specifically, financial liability of the institution is much lower for business customers than it is for consumers.

The Information Security Officer will keep an active Annual Customer Risk Assessment that not only inventories customers by the types listed above, but also keeps an inventory of the types of systems that each customer type typically uses.

We can then use these inventories and assessments to prioritize and target training and other risk mitigation activities to those customers and systems that represent the most risk.

Flyers and other Documents Available to Train Customers

The following flyers and documents are available to assist with customer awareness:

- Identity Theft Flyer
- Mobile Banking Tips and Trends
- New Account Disclosures
- Our Facebook Page
- Our LinkedIn Page
- Our Twitter Site
- Privacy Policy
- Remote Capture Deposit Setup Tips
- ACH Disclosures
- Bank Newsletter
- List other flyers, documents, etc. available

Laws and Regulations Related to Customer Awareness

It is important that all employees and management understand which laws and regulations require customer awareness training:

- Applicable Laws
  - BSA / AML
  - Children's On-line Privacy Protection Act (COPPA)
  - CTF
  - ADA
  - EFT Act (see Reg E below)
  - E-Sign Act
  - FACTA (and the Red Flags Rule)
  - GLBA
  - OFAC
  - UCC Article 4A
  - US Patriot Act (CIP and KYC)

- Applicable Regulations
  - Regulation B, Equal Credit Opportunity
  - Regulation CC, Availability of Funds and Collection of Checks
  - Regulation DD, Truth in Savings
  - Regulation E, Electronic Fund Transfers
  - Regulation M, Consumer Leasing
  - Regulation Z, Truth in Lending
  - 2005 FFIEC Guidance on Authentication (and the 2011 Supplement)

Policies and Other Documents Related to Customer Awareness

To help our customers respond to the risk exposure they experience, various policies, procedures, and other documents have been designed as non-technical controls and training materials which indirectly

affect our customers. These include:

- Telephone Authentication Procedures
- Authentication Risk Assessment
- Visitor Authentication Procedures
- Branchless Banking Management Procedure
- Identity Theft Flyer
- Commercial Customer Training Flyer
- Commercial Customer Training Checklist
- Training Games and Quizzes
- Vulnerability News Sources
- Policies Regarding the Disposal of Nonpublic Customer Information
- Incident Response Program
- Customer Identification Program
- Red Flags Program
- Remote Deposit Capture Procedure (and related documents and tools)
- New Customer Setup Procedures
- Public Presence Content Checklist
- Third Party Information Request Procedure

Customer Awareness Goals

Our customer awareness training addresses three different goals:

1. **Education:** This is the first training or notion as to what practices our customers should put into place. Some of this can be "mandatory," meaning that in order for the customer to use our system, the practice must be in place. An example of this would be password strength requirements to log into our online banking system.

   There are basic training requirements that should be met for all business customers. For customers using ACH or Wire Transfer, Remote Deposit Capture, and Business Bill Pay, as well as Wireless Banking, there are specific educational requirements.

2. **Active Motivation:** Whenever we deliver "reminder messages" to our customers, we should be adamant about explaining why. We must discover ways to motive customers to learn best practices ON THEIR OWN by activating their awareness of WHY our policies and procedures exist.

   Periodic reminders about security best practices, often delivered in the way we follow procedures ourselves, is the most effective method of Active Motivation. In other words, Active Motivation is the act of politely explaining to our complaining customers why our procedures and policies must be enforced. This should be done at the teller window, in our "old" media and "new" social media presence, and even in our alerts and warnings.

3. **Warnings:** Notifications of ongoing scams and new alerts or attack vectors in a manner that does not numb our customers against new information. In other words, we do not want warnings to work against activation, and thus we limit them to urgent and pertinent issues.

Education

The education process is the initial and ongoing contact with our customers to teach them about the risks they may face using information technology. Management should see the scope of our educational goals as being greater than centering our program on information assets. If we use our Facebook page to teach our customers how to protect themselves, they will come to our Facebook page when they need to understand one of our policies.

The [Information Security Officer / Compliance Officer] will continually find and/or create short, easy-to-understand messages that address the "Active Motivation" issue by helping customers understand the threat and thus the need to follow good practices. Agenda items for our customer education program may include:

- Provide risk-based training to our customers. During the Annual Information Technology (GLBA) Risk Assessment and also during subsequent "drill-down" risk assessments, the Information Security Officer will identify information that our customers need to know in order to protect themselves. For example, our Wireless Banking drill-down risk assessment identified information that customers should absorb into their body of knowledge. Educating customers on the dangers of smart phone usage provides timely information that can be included as posts on our [Facebook page. / social media sites.] Based on this premise, a series of posts can make evident the following:
    - A cell phone is like an electronic wallet or purse.
    - When a text message is sent, that text message is stored on the sender's cell phone, at least one server somewhere, and the receiver's cell phone. It will be around forever.
    - A cell phone is a computer that can make calls. Update it and protect it with antivirus software (AVS) like you would a computer.
    - If somebody steals a cell phone, what are they going to find?
- Our customers should be trained on the basics of information security. First and foremost, customers should know that NOT following good practices may cause them to lose money. Marketing efforts should be sure to tie the dollar directly to the message. Beyond that, messages should encourage customers to:
    - Always be on guard. Learn the threats, respect the threats.
    - Be aware of the value of the information they give out.
    - Install antivirus systems.
    - Turn on the firewall.
    - Update computers, laptops, and smart phones regularly.
    - Always back up important data.
    - Use their head and educate themselves!
- Customers must be taught how to use our "branchless banking" systems: our messaging should include subjects such as resetting passwords, using One Time Password/PIN (OTP) confirmations, changing their PIN, picking challenge questions, using the RSA tokens (for commercial customers), etc.

  - Whenever possible, vendor owners will determine if vendors make YouTube videos or other training information available for consumer use.

- Customers should be trained on how to create and use strong passwords, in addition to why they need to use strong passwords.
  - Our [Facebook page / social media sites] should link to "How to Choose Strong Passwords:" http://www.youtube.com/watch?v=COU5T-Wafa4
- Beyond passwords, all customers should be taught to:
  - Never respond to e-mails requesting personal or banking information such as Social Security numbers, bank account numbers or PIN numbers; and,
  - Refrain from clicking on any links in an e-mail if they are uncertain about the origin of the e-mail. Often times, links allow criminals access to the information through software programs that are invisible to the user.
- To mitigate legal risk, we will also provide awareness training as it pertains to Regulation E so that customers know what to look for, what to do, and what not to do as it pertains to their accounts. This training may include teaching our customers to:
  - Check their bank statements every month to ensure all transactions are valid and report suspicious activity immediately.
  - Never share their ATM or debit card PIN with anyone.
  - Never loan their ATM or debit card to anyone or they may become responsible for every transaction done by the third party. The same is true with checks.
  - Never give a signed blank check to anyone. Always fully complete the information, including the payee name, and don't leave any blank space on the written amount lines - line blank spaces out before and after the written amount.
  - Never provide personal or financial information to anyone who contacts them by e-mail (phishing) or by phone (pretext calling).

Business Customers Education

The [Information Security Officer / Compliance Officer], working with [Marketing / Operations / Branch Operations], will teach business customers the following important basics of business banking:

- The value of information and why protecting information is important.
- Never share login credentials with other employees. Any misuse of information or unapproved transaction initiation between employees using the same login credentials will be harder to ascertain and profile and puts the company at risk for loss;
- Ensure their company's computers are free from viruses and malware by keeping anti-virus software up to date.
- We will never contact a business customer and ask for credentials such as passwords, etc.
- We will always error on the side of identity theft and fraud prevention, and sometimes this means we prioritize the customers' protection a bit higher than convenience. We apologize in advance for when this does happen.
- To ensure that employees do not memorize login credentials in their browser.

- To never use sensitive information (such as tax ID number) as a password or user name.
- Only download programs or applications from trusted sources.
- Use secure websites for transactions and shopping.
- Always log off from any website and close their browser after making a purchase with your credit or debit card and close their browser when they are not using the Internet.
- What fees are associated with the customer's account and/or transactions.
- What constitutes fraud.
- Who to contact if they suspect fraud or malicious activity.
- Monitor their account regularly.

ACH and Wire Transfer Education

The [Information Security Officer / Compliance Officer], working with [Marketing / Operations / Branch Operations], will teach ACH customers our new authentication processes and that we will handle detection and response. We will also teach our ACH customers the following:

- What constitutes ACH fraud.
- That the fraud protection aspects of Regulation E does not apply to businesses, and what this means specifically in the event there is a fraudulent transaction (the business, and not the financial institution will be liable).
- They should monitor account activity on a daily basis. By using the Retail Online Banking or Commercial Online Banking service, they can view their account balances and transactions;
- They should implement a dual control system where appropriate. If one initiates ACH payments, one employee can create the transaction or batch and another employee can be required to approve it before release to the bank. This type of dual control helps minimize the risk of an employee having autonomous control over an entire process;
- The National Automated Clearing House Association (NACHA) will never ask for information from an account holder directly. They will always correspond through their bank membership rather than directly with a consumer or business.
- Detect and response procedures and how they could impact the timely transfer of funds.
- ACH / Wire Transfer customers should perform a risk assessment on a periodic basis to see where the customer faces the most risk with its ACH or Wire Transfer services.
- Appropriate disclosure documents required by the Compliance Officer (always check).
- What fees are associated with the customer's account and/or transactions.
- Who to contact if you suspect fraud or malicious activity.

Remote Deposit Capture Education

The [Information Security Officer / Compliance Officer], working with [Marketing / Operations / Branch Operations], will teach Remote Deposit Capture customers to use the web interface and scanners. We will also teach Remote Deposit Capture customers:

- What constitutes Remote Deposit Capture fraud.
- That the fraud protection aspects of Regulation E does not apply to businesses, and what this means specifically in the event there is a fraudulent transaction (the business, and not the financial institution will be liable).
- They should monitor account activity on a daily basis. By using the Retail Online Banking or Commercial Online Banking service, they can view their account balances and transactions;
- To properly protect / destroy NPI that is collected as a part of the Remote Deposit Capture.
- Other security best practices as a business customer. This may include limiting access to the Remote Deposit Capture equipment.
- Under what circumstances the account may be suspended.
- Remote Deposit Capture customers should perform a risk assessment on a periodic basis to see where the customer faces the most risk with its Remote Deposit Capture services.
- When funds will be available based on deposit timing.
- Appropriate disclosure documents required by the Compliance Officer (always check).
- What fees are associated with the customer's account and/or transactions.
- Who to contact if you suspect fraud or malicious activity.

On-line Banking and Business Bill Pay Education

The [Information Security Officer / Compliance Officer], working with [Marketing / Operations / Branch Operations], will teach Business Bill Pay customers to use the business online banking system, as well as the following:

- What constitutes fraud.
- That the fraud protection aspects of Regulation E does not apply to businesses, and what this means specifically in the event there is a fraudulent transaction (the business, and not the financial institution will be liable).
- Who is responsible in the event that a rogue employee uses business banking to commit fraud.
- Monitor account activity regularly.
- How to set up new users and disable users.
- Authentication practices and why they are important.
- Maintain up-to-date anti-virus, anti-spam, anti-spyware, and anti-malware programs.
- The timing related to on-line payments (when funds will come out of account, etc.).
- Always make it a point to clear the browsing history or cache.
- Appropriate disclosure documents required by the Compliance Officer (always check).
- What fees are associated with the customer's account and/or transactions.
- Who to contact if they suspect fraud or malicious activity.

Mobile Banking Education

The [Information Security Officer / Compliance Officer], working with [Marketing / Operations / Branch Operations], will teach Wireless Banking customers the following:

- The dangers of smart phone usage.
- To always store the mobile phone in a secure location.
- What constitutes fraud.
- Only download our app from our website or from a designated source.
- Not to memorize authentication credentials.
- To refrain from storing passwords on the mobile device.
- How to use power-on authentication.
- Use a PIN or password to keep your phone locked when it's not in use.
- Don't store information such as PIN numbers, passwords, account numbers, etc. on their phone.
- Make sure the phone doesn't automatically log into their bank account.
- For SMS banking: To save Name of Financial Institution's short number (xxxxx) in their address book so they recognize it and won't be fooled by spoof numbers.
- For SMS banking: To frequently delete text messages from Name of Financial Institution.
- To investigate remote wiping programs or services offered through providers.
- How to update smart phone operating system.
- How to require failure lockouts on authentication.
- How to purge text messages and e-mails that are no longer necessary (and why).
- To limit viewable e-mail to a day or two at the most.
- To use AVS on their smart phones.
- What smishing is, how it works, and how to protect themselves, and that the financial institution will never ask for sensitive information in text messages.
- (If consumer capture is being offered) To write "void" on captured checks.
- To keep Bluetooth turned off by default and use only when necessary.
- To make sure that Bluetooth is turned off when conducting any mobile banking transactions/inquiries.
- Remind customers of the dangers of jailbreaking (fraudulent apps and default root passwords).
- To regularly review statements via online banking.
- To discourage their children from letting others use their mobile phones.
- We will NEVER send e-mail upgrades to our mobile banking application.
- What fees are associated with the customer's account and/or transactions.
- Who to contact if they suspect fraud or malicious activity, including fraudulent applications that purport to be affiliated with Name of Financial Institution.
- To NOT rely solely on one channel: use online banking, mobile banking (both SMS and Mobile App) and maybe even visit the branch!

Active Motivation

The [Information Security Officer / Compliance Officer] is responsible for creating regularly scheduled security awareness reminders for inclusion on our [Facebook / LinkedIn / Twitter] site as well as newsletters, statement stuffers, and other customer messaging channels.

Through various channels including our [Facebook site / social media sites], we will periodically remind our customers about the risks they face and the safeguards that they should have in place. Our goal will

be to keep security of their information at the forefront of their thinking while using our information assets. Again, this can be done in person, electronically, or hard copy delivery.

One way we will approach this is to encourage our customers to learn on their own. Some ways we can do this include:

- Interactive teaching games from MindfulSecurity.com:
  - Beware of Spyware: http://onguardonline.gov/flash/spyware_loader.swf
- StaySafeOnline: http://www.staysafeonline.org/tools-resources/tip-sheets

We will also procure and hang posters at teller stations that remind customers of the importance of good information security practices.

- Posters such as "Work at Home Scams": http://my.infotex.com/consumer-fraud-advisor-continued-work-from-home-scams/
- Native Intelligence: http://www.nativeintelligence.com/ni-posters/index.asp
- SecurityPosters.net: http://www.securityposters.net/index.html

Active Motivation Messages

We must continually show our customers the different ploys that "bad guys" use to get their information or to perpetrate identity theft. Topics may include phishing, vishing and pretext calling. Examples of training materials we can use for this include:

- Creative, short best practice messages: http://m.infotex.com/vigilize
- Avoiding Online Scams: http://onguardonline.gov/articles/0001-avoiding-online-scams
- Avoiding Social Engineering and Phishing Attacks: http://www.us-cert.gov/cas/tips/ST04-014.html
- Computer Security: http://onguardonline.gov/articles/0009-computer-security
- Phishing: http://onguardonline.gov/articles/0003-phishing
- Phishing – Avoid the Bait: http://onguardonline.gov/flash/phishing_loader.swf?fileToLoad=http://www.onguardonline.gov/flash/phishing.swf

Using Ongoing Scams: We will try to integrate the "why component" into our warning messages. Thus: "never click on a link sent from us" could be accompanied by a recent notification that there is a fake FDIC phishing message in the e-mail sphere. There are many sources for these alerts, and signing up for the Infotex mailing list is just one way to "get connected" to the real-time stream of information about ongoing scams.

- Infotex Mailing List: https://my.infotex.com/mailing-lists-2/
- Consumer Advisories: http://www.ic3.gov/media/2010/WorkAtHome.pdf
- Consumer Threat Alerts: http://home.mcafee.com/consumer-threats-signup

- OCC Consumer Advisories: http://www.occ.treas.gov/news-issuances/consumer-advisories/2011/index-2011-consumer-advisories.html
- US Cert: http://www.us-cert.gov/nav/nt01/

Challenge Our Customers: Just as we are teaching our employees our Red Flags program and ways to spot fraudsters and suspicious activity, an effective program will challenge customers to look for those signs that indicate fraudulent activity. We will be considering on-line games, contests, and other activities to create this challenge.

Targeted Training: The Information Security Officer, working with [the IT Steering Committee / Branch Operations / Marketing] will create a customer risk assessment that separates high-risk customers from low risk customers (both consumer and commercial). Training will be targeted to customers based on risk and use.

Vulnerability Announcements

The Information Security Officer will develop reliable sources for reporting day zero exploits, ongoing attacks, and new vulnerabilities. The Information Security Officer is responsible for filtering such sources down to those which would pertain to the customer. The Marketing Director will choose which of these messages warrant posting on the institution's [Facebook / LinkedIn / Twitter] site.

It is important that we keep our warning system separate from our ongoing "active motivation" system. We will keep our customers informed about ongoing scams so they can be on guard. However, we must be VERY careful how we do this so that we're not dulling their sensitivity to issues as they arise. Our approach to customer awareness training MUST consider the fact that our customers are bombarded with information all day long, and our warnings must cut through all the noise and GRAB YOUR CUSTOMERS' ATTENTION.

We will only use the WARNING capability of our communication channels (web alerts, text messaging, social networking sites) when there is a direct, imminent threat to our customers.

Broadcast Awareness: Security Warnings

Name of Financial Institution defines "imminent threats and/or vulnerabilities" as those ongoing incidents that are pertinent to our customers, could cause damage to our customers, and are actually in progress. For example, the dangers of phishing is not an imminent threat. However, an imminent threat would be when a phishing site is discovered with our institution's website being spoofed, and customers complain about an e-mail linking to that site.

In the event that an incident requires "broadcast awareness" of imminent threats to our customers, procedures will be followed that are maintained in the institution's Incident Response Plan. The Information Security Officer may work with Marketing to utilize social media, as well as encourage employees to utilize their own social networking tools, to broadcast awareness.

We will be considering new methods of approaching this include leveraging our SMS banking database to distribute warnings via text messaging, as well as the use of Facebook, Twitter and other social

networking sites. We are also considering allowing their employees access to Facebook and other social networking sites. When the time is appropriate, we may consider using a broadcast e-mail asking our employees to "like" carefully written posts about recent attacks on our institution.

We must avoid desensitizing our customers with a steady trickle of benign warnings. As incoming notifications of ongoing threats, attack vectors, and scams arise; the Information Security Officer will consider including them as part of our Active Motivation message stream, delivering the WHY part of the message, and excluding them from our warning system.

The following sources will be used to distribute Warnings as defined in this strategy:

- Alert on our web page
- Post on Facebook
- Tweet on Twitter
- Media Calls to ([list media sources and phone numbers here]
- Press Release sent to ([list media sources and phone numbers here]

Notification to Customers of Security Breaches

Note: The following should merely reflect your Incident Response Policy. Be sure to check this against your existing policy.

The [CIRT / IRT / Steering Committee] will classify all incidents into one of three types:

- Disclosure Incidents: These are incidents which, because of some statute or regulation, require [name of financial institution] to notify customers, law enforcement, examiners, or the board of directors. The [CIRT / IRT / Steering Committee] must comply with all applicable laws and regulations, including state laws such as [Indiana Code 24-9.4 / applicable law in your state] and the FFIEC's Financial Institution Letter 27-2005.
- Security Incidents: These are incidents related to the confidentiality and integrity of information. They can include technical incidents such as malware (virus, worm, and trojan horse) detection, unauthorized use of computer accounts and computer systems, but can also include non-technical incidents such as improper use of information assets as outlined in the Acceptable Use Policy.
- Negative Incidents: These are incidents related to the availability of information assets or other risks such as legal risks, strategic risks, or reputational risks that do not directly impact the confidentiality or integrity of information. For example, installing an unlicensed application on a bank-owned application does not impact confidentiality, integrity, or availability, but this policy still requires the [CIRT / IRT / Steering Committee] to track it.

The [CIRT / IRT / Steering Committee] may develop a severity classification system within each incident type. The Information Security Officer to report all Notification Incidents to the Board of Directors as they occur, and report [severe / critical] Security Incidents and [critical / severe] Negative Incidents as deemed necessary by the [CIRT / IRT / Steering Committee] in real time.
The Information Security Officer is authorized to classify incident types, as defined above, as well as incident severities. All incidents should be summarized by type and [criticality / severity] in the Annual Report to the Board.

The Information Security Officer will notify the Board of Directors of all Disclosure Incidents "in real time." The Board of Directors will also be notified "in real time" anytime an incident is considered to be critical in severity.

All suspected and/or confirmed instances of attempted and/or successful intrusions must be immediately reported according to the Incident Response Plan. The Incident Response Plan will address regular reporting requirements for analyzing trends, performing "post-mortem analysis" of past incidents, and other requirements as determined by the [CIRT / IRT / Steering Committee].

The [CIRT / IRT / Steering Committee] will create and document Notification Requirements in the Incident Response Plan that establishes guidelines for reporting incidents to management, to the Board of Directors, to law enforcement, to customers, and to the media in a manner consistent with all applicable laws as well as the bank's risk management policies and procedures.

Delivery of [Privacy Policy / Privacy Statement / Online Customer Privacy Notice]

The Branchless Banking Policy has specific instructions related to the delivery of our [Privacy Policy / Privacy Statement / Online Customer Privacy Notice]. We will deliver to our customers a copy of our [Privacy Policy / Privacy Statement / Online Customer Privacy Notice] whenever required by law or regulation, and whenever customers sign up to use new branchless banking assets. An inventory of assets and when a Privacy Policy disclosure is required is kept in the Authentication Risk Assessment. To be safe, management should get in the habit of including a Privacy Policy in any and all customer awareness training exercises.

Name of Financial Institution will provide periodic update awareness advisories regarding online privacy issues, our Privacy Policy, and our efforts to ensure that proper controls are in effect. The [Information Security Officer / IT Steering Committee / Compliance Officer] will ensure that these notices are provided as needed. Specifically, they should go out at least once per year, or whenever there are major changes in controls, threats, or customer types.

Concluding Sections

The following sections may or may not apply to your institution, depending upon your own policy/procedure development protocols. However, we do strongly urge you to include the distribution list, policy owner, and policy reviewers section for your convenience and to ensure appropriate review and training. Please remove this section.

Contribution to Control Objectives for Information Technology

Following this strategy contributes to the achievement of CobiT 4.0:

- PO6: Communicate management aims and direction.
- PO7: Manage IT human resources.
- DS7: Educate and train users.

Strategy Owner

- Title Here

(Note: If you document the strategy owner in the header, this section would be redundant and may be removed.)

Strategy Reviewers

- Titles Here

Distribution List

The following positions will receive this policy and any changes to this policy:

- Information Security Officer
- Compliance Officer
- Marketing Director
- Operations
- Senior Management and Management Team Members (as listed in the Awareness Training Procedure)
- List other individuals. Consider establishing an e-mail alias corresponding to the individuals.

Storage of Policies, Procedures and Standards

The Information Security Officer is responsible for maintaining current copies of all information security related policies and procedures. These will be stored [state method and location] and an electronic copy will be stored off-site [state location]. The electronic copy will be updated annually (in December) as well as on an as-needed basis any time there is a major revision of a particular policy or procedure.

Related Policies / Procedures / Tools

- Awareness Training Procedure
- Customer Identification Program
- Identity Theft Prevention Flyer
- On-line Banking Critical Elements Checklist
- Commercial Customer Awareness Training Checklist (Risk Analysis)
- Commercial Customer Awareness Flyer
- Consumer Awareness Flyer
- Customer Banking Product Controls

- Mobile Security Puzzle
- Opt-out Agreement
- Public Presence Checklist
- Social Media Development Standards