# The Customer Awareness Control

## Executive Summary:

Within the context of your existing Awareness Training Program, the new FFIEC Supplement requires that you focus on customer awareness controls. Meanwhile, every risk assessment related to wireless banking results in identifying the need for more customer awareness. This White Paper brings everything that can be done to assist in this effort into one place. To summarize:

- Risk Assessments:
    - Risk assessments should identify which customer controls should be promoted, in order of risk.
    - Risk assessments should also identify "high risk customers" beyond your commercial customers.
- Integration:
    - Customer awareness should be integrated in all communications.
    - "Old" media and social media and mobile banking messages should be used in the process.
    - Customer Awareness should be considered in all aspects of the Information Technology Governance Program.
- Objectives:
    - The Customer Awareness Program should achieve three objectives:
        - Education: material should teach customers good practices.
        - Active Motivation: all communications with customers should teach "why." It's as simple as explaining our policies and procedures, and why they exist.
        - Warnings: we must have a mechanism in place to communicate ongoing issues.
    - Compliance: Between now and your next examination, you should develop a Customer Awareness Strategy.

We recommend that all management team members of the bank read this White Paper as a first step in the process.

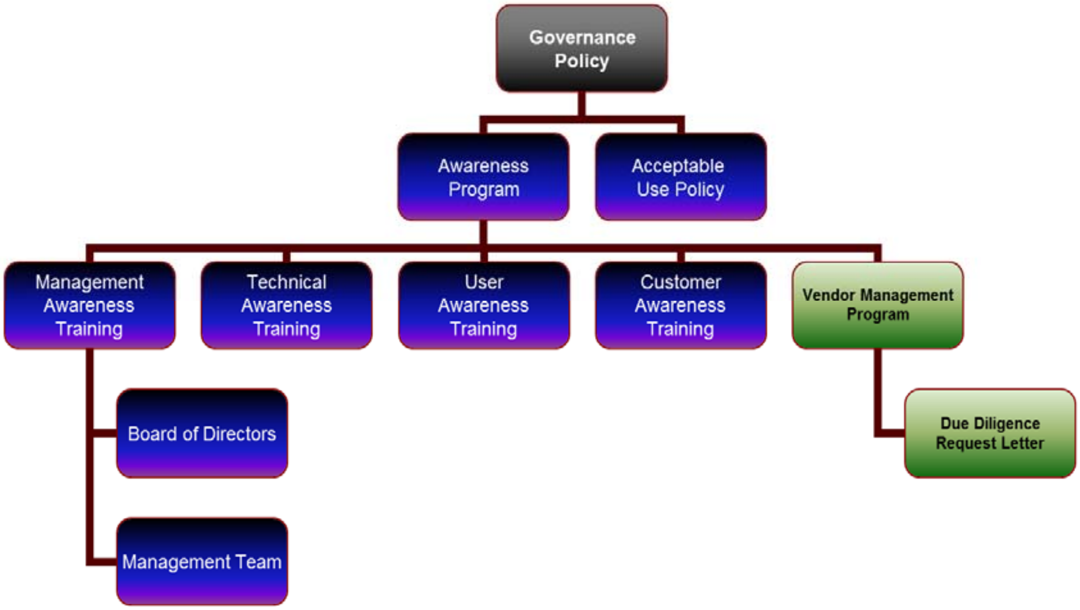
### Your Customer Awareness Program

As a financial institution, you know how important information security is to your organization. You follow regulations regarding annual security awareness training for your employees. You cover the importance of creating strong passwords and keeping those passwords secure. Employees learn what constitutes proper authentication and authorization techniques and what questions to ask before releasing nonpublic information. Employees are taught how to spot a phishing e-mail and not to click on a link in an e-mail that wasn't expected. You document that your employees attend the annual training and examiners confirm that the training is taking place. Your employees are on the frontline and are armed with "awareness."

But what about your customers? They use your on-line banking assets and now mobile devices that access nonpublic information via several mobile channels (mobile web, sms, and mobile applications). They too risk receive phishing e-mails and pretext calls, and it gets worse in the mobile environment.

### Context

We have traditionally viewed Customer Awareness training as a component of an overall "Awareness Program" that is required by policy at the board level, and works side by side with awareness training provided to our management team, technical staff, and general users. We've even gone so far as to declare that awareness training in general works through other Information Technology Governance programs, such as vendor management, when we specify requirements or, more effectively, when we explain why our policies and procedures exist. For example, the e-mail we send to our vendors asking them to comply with our vendor due diligence process works better if we "blame the regulators," but *much* better if we help our vendors understand why the program exists in the first place.


Governance Policy
Awareness Program
Acceptable Use Policy
Management Awareness Training
Technical Awareness Training
User Awareness Training
Customer Awareness Training
Vendor Management Program
Board of Directors
Management Team
Due Diligence Request Letter

As we start to take our Customer Awareness Program to the next level, we must recognize that customer awareness touches upon most areas of governance, including access management, incident response, asset management, business continuity, risk management, and yes, even vendor management, as we begin to outsource some of the "help desk" functionalities inherent in newer technologies. Just one example of this is the extremely important need for us to apply the monitoring function of Incident Response towards our roll-out of mobile banking; and use this process to continually update the tools we make available to front-line employee. When a customer comes in excited that they just purchased their brand new Galaxy Tab and they do not realize it's powered by Android, our employees must be able to go to some sort of chart that needs to be updated as new devices are put into the market place. Unless we want to create an entirely new ad hoc process to address this problem, the best process already in place for this is our Incident Response program.

### FFIEC Supplement

On June 28, 2011, the Federal Financial Institutions Examination Council (FFIEC) issued a Supplement to the Authentication in an Internet Banking Environment guidance issued in October 2005. That supplement addresses the need for raising customer awareness of potential risks and identifies certain specific minimum elements that should be part of an institution's customer awareness and education program. Not only should the institution work to educate retail customers, but commercial customers as well.

According to the Supplement, the financial institution's customer awareness and education program should 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.

### Regulation E

Regulation E defines the protections given to consumers to protect them from electronic fraud, and financial institutions and companies processing electronic items must follow the rules it states. Not only do the rules protect consumers, they help financial institutions and companies conduct proper investigations of claims prior to making reimbursements in order to protect themselves from losses as well. If you look at the basics of Regulation E, it says if the customer advises his financial institution promptly about suspicious activity, he will not be held accountable for erroneous charges to his account.

### Risk Assessments

The Supplement to Authentication in an Internet Banking Environment indicates that financial institutions should review and update their existing risk assessments as new information becomes available, prior to implementing new electronic financial services, or at least every twelve months. That's fine for the institution, but what about your customers? The Supplement recommends that you make your commercial online banking customers aware of the need to perform a related risk assessment and controls evaluation on a periodic basis. What risks do they face using the online banking system? What about Electronic Funds Transfer (EFT), Automated Clearing House (ACH), or wire transfer services? What controls should they implement to keep their information secure? In addition, you should ensure that your commercial customers are aware of and manage the risks inherent with Remote Deposit Capture (RDC). Help them to understand the risks (e.g. processing errors, unauthorized activity) and what controls can be put into place to mitigate those risks.

Consider identifying "high risk customers" to target more expensive training. Meanwhile, almost every risk assessment related to "branchless banking" results in the fact that the primary control to mitigate risk is Customer Awareness Training. This applies to both Smart Phones and Tablets (i.e.: iPads, Slate, Xoom, etc.)

**Controlling Risks**

The Supplement recommends that you help your customers become aware of alternative risk control mechanisms that they may consider implementing to mitigate their own risk, or alternatively, a listing of available resources where such information can be found. Teach your customers that they can go directly to YOU (or your Internet banking site) for security alerts or the latest threats. Prepare a handout or statement stuffer that teaches your customers about the need for using strong passwords. Explain to your customers why you are implementing stronger layered security (e.g. “out of wallet” and “red herring” questions, out-of-band authentication, etc.). Also, teach your customers about phishing and pretext calls, while instilling in them the need for proper authentication of callers. Offer your customers a way to further educate themselves and control their own risks by providing additional reading material.

In April 2011 **infotex** made available a flyer entitled “Mobile Banking Tips and Trends” that you are welcome to use as a starting point in your objective to “get the word out.” We are seeing banks successfully include each of the messages in this flyer in their social media presence (particularly through their Facebook page).

**Contact Information**

If your customers notice suspicious account activity or experience security-related events, they need to know who to call. You should make readily available names and phone numbers of key employees that can handle calls of that nature. Show your customers where to get that information quickly on your Internet banking site. Provide business cards or other written notification options that can be readily available. This will decrease the impact of fraudulent account activity, and has reputation and legal risk mitigation benefits.

In addition, your customers should be aware of various organizations that they may contact if they suspect that they have become victims of identity theft. Here are just a couple of options:

- Internet Crime Complaint Center: http://www.ic3.gov/default.aspx
- Fight Identity Theft Brochure: http://www.occ.treas.gov/news-issuances/bulletins/2004/bulletin-2004-42a.pdf
- Privacy Rights Clearinghouse: Federal Trade Commission - What To Do If Your Personal Information Has Been Compromised: http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt150.shtm
- Fighting Back Against Identity Theft: http://www.ftc.gov/bcp/edu/microsites/idtheft/

**Awareness / Training Delivery**

Many channels are available to deliver your training and awareness programs to your customers. Statement stuffers, links back to information on your Internet banking site and e-statements are typical in most banks these days. Some financial institutions hold a special “customer appreciation” event, with a talk dedicated to information security. Attendance at these is high, and most of the attendees are retired people.

Take advantage of the many different games, awareness training sites, and on-line educational materials produced by third parties, and consider linking to them from your social networking sites (e.g. Facebook, Twitter). For your commercial customers, webinars, slideshare presentations (http://en.wikipedia.org/wiki/SlideShare) on LinkedIn or YouTube videos are methods of delivering the awareness messages on-line that many institutions are trying.

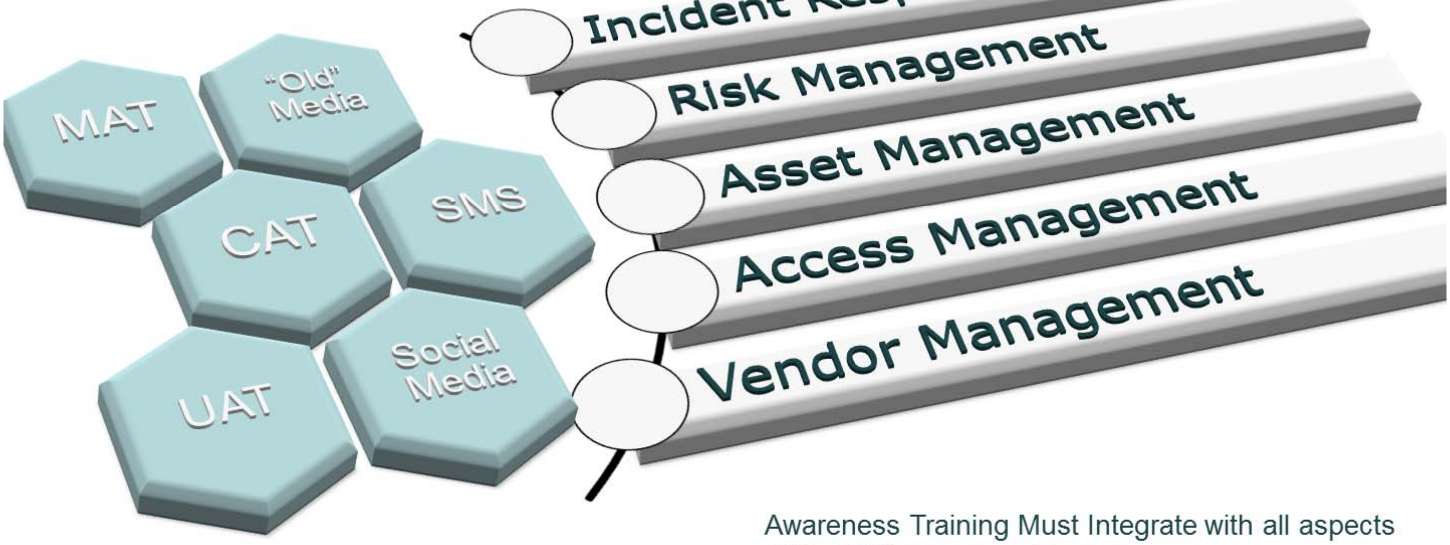
It is important to document all the ways you deliver awareness messages to your customers. Doing so will substantially lower the impact of incidents caused by poor customer security practices. For example, if you continually warn your customers to use power-on authentication on their smartphones and to purchase the remote wipe service you're reselling in your lobby and from your website, when they come into the bank upset that they lost their smartphone with $100 in wallet capabilities, you will be in a much better position IF you have documented your attempts to educate your customers.

Consider the use of "new media" . . . . as if e-statements and websites are old. The advent of Facebook, Twitter, and SMS banking offers a LOT of opportunity when it comes to getting the message out. Imagine the power of the "Seven Degrees of Separation" sometimes referred to as the Kevin Bacon Game when it comes to getting the word out that there is a phishing attack on your bank. If you can tap into your own employee's Facebook friends, your alert can "go viral." As powerful is the opportunity afforded by text banking (SMS). If you can send alerts about a smishing attack (a phishing attack using text messaging) to all mobile banking customers, you will beat the attackers before your customer sees their message!

### Integration

This brings us to the most important aspect of any customer awareness training program. It must be integrated, not only with other areas of the awareness program, but also with all aspects of your IT Governance Program.

Customer Awareness Training (CAT) must integrate with User Awareness Training (UAT) and Management Awareness Training (MAT).



Awareness Training Must Integrate with all aspects of the IT Governance Program.

Like any other "integration project," this is much easier said than done. The most important thing you can start doing is raising the question, at every step of the IT Governance way, "how can we integrate this with customer awareness training." Beyond the legal risk mitigation benefits of having a nice paper trail that you've done all you could, it's the only way you are going to get the message out to every single customer.

When we see banks design customer awareness organically into their every approach, we see ideas such as "why you should not memorize credentials" text messages go to the user that just made that choice when they registered for the mobile banking app. You might respond with "well that depends on the mobile banking app," and we say "yes, exactly, which is why you should raise the issue there too."

**Objectives and Approach**

To fully understand what we need to accomplish in order to achieve not just compliance value, but also true security value, it helps to compare our goals when training our own employees to the goals we have when training our customers.

Awareness Goals for Our Employees: User Awareness Training has three primary goals:

1. Education: Teach our users policies and procedures, and confirm that they understand the information that we teach them. What we teach them is based upon risk, and we want to be sure they understand the control in place that mitigates the most risk, as well as the vulnerabilities they face as users. And for compliance and security reasons, training is mandatory and documentation imperative.
2. Motivation: As almost every audit report shows, the disciplinary program for policy violation is not enough motivation. Though in theory our employees should be motivated to follow policy and procedure, we've found that helping users understand WHY controls are in place makes it easier for them to not only cooperate with the controls, but roll up their sleeves and learn the most effective application of the controls. Thus, our User Awareness Program must continually draw a connection between controls and why the controls exist.
3. Activation: Even if we know the policy, because we are continually bombarded with transactional information requiring decisions on a day-to-day, minute-to-minute basis, we must activate our users' awareness through the use of reminders that draw the connection between controls and why the controls exist. We need to overcome a sense of "techno-hypnosis." More importantly, we must continually test those controls that mitigate the most risk so that employees find ways to make following procedure a natural part of their day-to-day and minute-to-minute response to potential vulnerability exploits. For example, most social engineering attacks are based on methods to gain user trust while simultaneously leveraging users' goal/motivation to provide friendly, polite service. Continual testing not only increases compliance motivation, but it also gives our employees a chance to find ways to politely follow procedure (rather than sidestepping procedures to be polite). One of the easiest ways to activate user awareness is by sharing ongoing scam/fraud stories. People like to read these stories, it gets them talking about it, and it helps pass the information along to our customers.

The above framework for understanding the goals of training our employees obviates the challenges we face in creating a customer awareness training program. We can't fire our customers for violating policy, we can't test our customers, and there is no mandatory training requirement in order to remain a customer.

But it also helps to identify what is SIMILAR between teaching our employees and teaching our customers. Though motivation can't be based on a "do it or we'll fire you" premise, our customers will still be motivated if they understand WHY a practice protects them.

Meanwhile, maybe we CAN make training mandatory in some situations as part of the agreements we initiate with our customers. For example, we can lace awareness messages into normal procedures. We're already doing this if our Internet banking is configured to require strong passwords. If the feedback we give a customer that doesn't use a strong password can include WHY the bank needs customers to use strong passwords, we're now motivating our customer. And, if the authentication process is designed correctly, we can not only inform our customer, but we can collect documentation that the customer received the message.

Another example: consider requiring commercial customers to complete a quick survey that includes awareness questions that will help us identify information to provide to them that will address their misconceptions about information security. The survey can also help us complete a risk profile on our customers so that we can target additional awareness training to high-risk customers in the future.

Another similarity between user and customer training includes the fact that we can still use the WHY factor to motivate compliance with policies and procedures. The most important introductory phrase your help desk and front-line employees should learn is: "For your protection." But beyond explaining that our procedures exist for the protection of the financial institution and our customers, if we drill down a bit to help customers understand why certain procedures are in place, they will be more cooperative with those procedures. (We all take our shoes off in an airport without too much disgruntlement because we all remember the shoe bomber.)

Customer Awareness Goals: Because of these differences and similarities, our customer awareness training addresses three very similar yet slightly different goals:

1. **Education:** This is the first training or notion as to what practices your customers should put into place. Again, some of this can be "mandatory."

2. **Active Motivation:** We recommend combining "activation and motivation" into one objective for customers, because unlike our employees, the act of increasing our customers guard is indeed the act of motivating our customers. Including activation and motivation in one process speaks to the fact that whenever we deliver "reminder messages" to our customers, we should be very 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 social media presence, and even in our alerts and warnings.

   One great example of how we've seen this at work is a Facebook post by a Client. The bank was under a phishing attack. Not only did they use "old media" methods of getting the word out (radio, e-mail, web site warnings) but they also designed a message and requested that each of their employees post it on their own Facebook page. In the message was a link to a YouTube video about how to spot a phishing message. The message also started with the phrase "Your money could be stolen." Of course, the bank had a policy allowing employees to access Facebook.

3. **Warnings:** Notifications of ongoing scams, 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.)

**Education**

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

Curriculum: We suggest that your awareness program choose 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 your customer education program may include:

- Provide risk-based training to your customers. During your annual risk assessments and drill-down risk assessments, you should be identifying information that your customers need to know in order to protect themselves. For example, our Wireless Banking drill-down risk assessment identified plenty of information that customers should absorb into their body of knowledge. Educating customers on the dangers of smartphone usage provides timely information that your customers will love you for, and you can provide this education in your social media sites. Based on this premise, your customers should be made aware of the following:
    - Your cell phone is like an electronic wallet or purse.
    - When you text somebody, that text message is stored on your 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 your cell phone, what are they going to find?
- Your customers should be trained on the basics of information security. First and foremost, customers should know that NOT following good practices will cause them to lose money. As seen above, 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 anti-virus systems.
    - Turn on their firewall.
    - Update their computers, laptops, and smartphones regularly.
    - Always back up important data.
    - Use their head and educate themselves!
- How to use your systems: resetting passwords, using One Time Password/PIN (OTP) confirmations, changing your PIN, picking challenge questions, using the RSA token.
    - Find out if your vendors have YouTube training videos. Link to them from your web page or your social networking sites. Ideally, your smartphone application will link out to awareness training materials.
- Your customers should be trained on how to create and use strong passwords, in addition to why they need to use strong passwords.
    - 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 help protect yourself and your customers, you should also provide awareness training as it pertains to Regulation E so they know what to look for, what to do, and what not to do as it pertains to their accounts. This training may include teaching your 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 a third party who contacts them by e-mail (phishing) or by phone (pretext calling).

<u>ACH Training</u>: The supplement requires teaching your ACH customers your new authentication processes and how you are going to handle detection and response. You should also be sure to teach your ACH customers to:

- 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;
- 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;
- 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.
- Remind your customers that 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.

The above information is a guide. There's numerous other ways of training your customers. Of course, you can create your own documentation and post it on your Internet banking site, hang posters at teller stations, incorporate your customer training into your social media presence such as your Facebook page, YouTube, Twitter, and LinkedIn. It doesn't matter how you do it – but that you do it!

**Active Motivation**

You should periodically remind your customers about the risks they face and the safeguards that they should have in place. Keep security of their information at the forefront. Again, this can be done in person, electronically, or hard copy delivery.

One way to approach this is to encourage your customers to learn on their own. Some ways financial institutions are doing this include:

- Interactive teaching games from MindfulSecurity.com:
  - Identity Theft Faceoff : http://onguardonline.gov/flash/IDTheft_loader.swf?fileToLoad=http://www.onguardonline.gov/flash/IDTheft.swf
  - Beware of Spyware: http://onguardonline.gov/flash/spyware_loader.swf
- Posters such as “Work at Home Scams”: http://my.infotex.com/?p=2480
  - Native Intelligence: http://www.nativeintelligence.com/ni-posters/index.asp
  - SecurityPosters.net: http://www.securityposters.net/index.html
- StaySafeOnline: http://www.staysafeonline.org/tools-resources/tip-sheets

Active Motivation Messages: The different ploys that “bad” guys use to get their information or to perpetrate identity theft. Topics may include phishing, vishing and pretext calling. Here are some training materials:

- 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: Try to integrate what you may be tempted to put into your warning program into the active motivation program as the “why component” of your message. 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: http://my.infotex.com/?page_id=1557
- 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 Your 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. Some of our Clients are considering on-line games, contests, and other activities to create this challenge.

Targeted Training: An effective approach to Active Motivation would include a risk assessment on customer types and developing methods to target training towards those customers needing it the most. Why waste money sending statement stuffers to customers who are not enrolled in your on-line banking system? Would it be better to distribute that information in the e-statements? Which customers present the most risk, and as importantly, which customers will be more receptive to the information. Why develop a webinar for Millennials when a face-to-face seminar with your retirees will be well-attended?

### Warnings

Your bank should already have a warning process in place that allows you to convey real-time information to as many customers as possible and as quickly as possible. New methods of approaching this include leveraging your SMS banking database to distribute warnings via text messaging, as well as the use of Facebook, Twitter and other social networking sites.

Some of our clients are working towards a more liberal social media policy in their financial institutions. They are considering allowing their employees access to Facebook and other social networking sites. Part of this is due to the fact that we know they are visiting those sites anyway, going around our "network controls" with their own smartphones. Some clients are weighing the security and productivity concerns of this consideration against the opportunity for quick warning distribution (as well as marketing messages, we admit). In other words, imagine a broadcast e-mail asking your employees to post carefully written language about the bank's recent phishing attack on their own Facebook page?

Your customers should be informed about ongoing scams, new alerts or attack vectors 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 must avoid desensitizing our customers with a steady trickle of benign warnings. Thus, as you receive incoming notifications of ongoing threats, attack vectors, and scams; consider including them as part of your Active Motivation message stream, delivering the WHY part of the message, and excluding them from your warning system.

Only use the WARNING capability of your communication channels (web alerts, text messaging, social networking sites) when there is a direct, imminent threat to your customers. For example, warning your customers of the fourteenth FDIC phishing scam this month will do nothing to put them on guard. But if when we are being phished the SMS your customers get is the first they've received in several months, they will be more apt to pay attention to the warning.

### Immediate Compliance with the Supplement

It is our understanding that between now and the beginning of January 2012, you should be developing a multi-disciplinary, risk-based Customer Awareness Strategy. This can be documented as simply as a half-page explanation of the strategy that you intend to implement to bring your financial institution into compliance with this part of the Supplement. However, you should be following through with actions and doing everything you can to collect evidence of the efforts you are making to educate, activate, motivate, and warn your customers. Doing so will not only help you from a compliance perspective, but it will also lower the impact of any customer-related fraud and/or security incidents.

You should also already be updating your E-banking Policy to include more specific objectives for management (to inventory all branchless banking assets, conduct a risk assessment to identify critical assets and transactions needing more robust authentication as well as detect and response mechanisms, conduct triggered risk assessments in real time from now on). The policy also needs to be updated to require a documented Customer Awareness Training strategy as well as documentation of efforts made by the bank to deliver this training.

### Do Not Call List

Many people have, with the implementation of the National Do Not Call Registry, registered their phone numbers on the Do Not Call list. However, there are exemptions to that rule. One in particular exempts an organization from the rule if there is an existing business relationship with the consumer. However, if your customer asks you not to call, then you may not call the customer, even with the established business relationship. That customer should then be put on your own Do Not Call list. Help your customers to become aware of this, and alert them of what circumstances that they may be contacted.

### Long Term Compliance with the Supplement

As important as developing a method of delivering training material, as important as fine-tuning your method of quickly and widely distributing warning materials, as important as keeping the risk-based list of active motivation messages and tying them to ongoing scams, is the important task of keeping solid documentation of your efforts to educate, motivate, and warn your customers. This documentation will not only be important as your auditors and examiners start testing your compliance with the supplement, but we believe it will truly mitigate legal risk and financial impact.

If your institution is adequately complying with the customer awareness component of the Supplement, over the long run you will substantially reduce risk as the impact of customer incidents. And yes, we truly believe that in time the likelihood of customer incidents will come down. Eventually, those customers who stubbornly refuse to take advantage of your efforts will experience their own incident. We’ve found, as described in testing above, that this is all it takes to achieve true motivation!

### The First Step: Management Awareness

As stated above, we believe that “integration” becomes paramount when it comes to Customer Awareness, meaning that the notion of “explaining risks and controls to our customers” should integrate with our social media presence, with other areas of our IT Governance Programs, with our SMS banking (tips, alerts, and warnings) . . . practically everything we do now should exude customer awareness.

But that needs to start with our employees. In other words, we need to make sure our employees are aware of the awareness we provide to our customers. Not only do we want our employees to understand the same best practices we are teaching to our customers, but if we can rely on them to get the word out, we will achieve the objective most effectively.

And employee awareness really starts with management awareness. In other words, if you haven’t already done so, send this article to your management team!

**infotex** *is a technology risk management firm specializing in auditing, controls development, and managed security services. Ask us about our new ELM Compliance system!*