Thrift Bulletin
TB 83

This rescission applies to the transmitting document only and not the attached interagency guidance. Refer to OCC 2003-15 for the status of the attached interagency guidance.

Handbooks: Thrift Activities; Compliance Activities
Subjects: Technology Risk Controls; Electronic Banking Sections: 341; 370

Interagency Guidance on Weblinking: Identifying Risks and Risk Management Techniques

Summary: Attached is Interagency guidance on Weblinking. Agencies adopting this guidance include: Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision.

For Further Information Contact: Your Office of Thrift Supervision (OTS) Regional Office or the Supervision Policy Division of the OTS, Washington, DC. You may access this bulletin at our web site: www.ots.treas.gov.

Thrift Bulletin 83

A large number of financial institutions maintain sites on the World Wide Web. Some websites are strictly informational, while others also offer customers the ability to perform financial transactions, such as paying bills or transferring funds between accounts.

Virtually every website contains "weblinks." A weblink is a word, phrase, or image on a webpage that contains coding that will transport the viewer to a different part of the website or a completely different website by just clicking the mouse.

While weblinks are a convenient and accepted tool in website design, their use can present certain risks. Generally, the primary risk posed by weblinking is that viewers can become confused about whose website they are viewing and who is responsible for the information, products, and services available through that website.

The purpose of the attached guidance is to assist financial institutions in identifying risks posed by the use of weblinks on their websites and to suggest a variety of risk management techniques institutions should consider using to mitigate these risks. This guidance applies to institutions that develop and maintain their own websites, as well as institutions that use third-party service providers for this function.

Attachment

Scott M. Albinson

—Scott M. Albinson
Managing Director, Supervision

Federal Deposit Insurance Corporation
National Credit Union Administration
Office of the Comptroller of the Currency
Office of Thrift Supervision

WEBLINKING: IDENTIFYING RISKS AND RISK MANAGEMENT TECHNIQUES

A. RISK DISCUSSION

Introduction

A significant number of financial institutions[1] regulated by the financial institution regulatory agencies (Agencies)[2] maintain sites on the World Wide Web. Many of these websites contain weblinks to other sites not under direct control of the financial institution. The use of weblinks can create certain risks to the financial institution. Management should be aware of these risks and take appropriate steps to address them. The purpose of this guidance is to discuss the most significant risks of weblinking and how financial institutions can mitigate these risks.

When financial institutions use weblinks to connect to third-party websites[3], the resulting association is called a "weblinking relationship." Financial institutions with weblinking relationships are exposed to several risks associated with the use of this technology. The most significant risks are *reputation risk* and *compliance risk.*

Generally, reputation risk arises when a linked third party adversely affects the financial institution's customer and, in turn, the financial institution, because the customer blames the financial institution for problems experienced. The customer may be under a misimpression that the institution is providing the product or service, or that the institution recommends or endorses the third-party provider. More specifically, reputation risk could arise in any of the following ways:

---

[1] The Agencies intend this guidance to apply to the following institutions: insured state non-member banks, national banks, insured state branches of foreign banks, federal branches of foreign banks, federal and state chartered credit unions insured by the NCUA, savings associations, and any subsidiaries of such entities (except functionally regulated subsidiaries including SEC regulated securities brokers/dealers, investment companies and investment advisors and state insurance regulated entities).

[2] Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision.

[3] This guidance applies to links to third parties that offer products, services, or information directly to financial institution customers. It does not apply to operational links from a financial institution's website to a third-party service provider that is providing services on behalf of the financial institution, *e.g.*, a link to the institution's Internet banking service provider.

- customer confusion in distinguishing whether the financial institution or the linked third party is offering products and services;
- customer dissatisfaction with the quality of products or services obtained from a third party; and
- customer confusion as to whether certain regulatory protections apply to third-party products or services.

Compliance risk arises when the linked third party acts in a manner that does not conform to regulatory requirements. For example, compliance risk could arise from the inappropriate release or use of shared customer information by the linked third party. Compliance risk also arises when the link to a third party creates or affects compliance obligations of the financial institution.

Financial institutions with weblinking relationships are also exposed to other risks associated with the use of technology, as well as certain risks specific to the products and services provided by the linked third parties.[4] The amount of risk exposure depends on several factors, including the nature of the link.

Any link to a third-party website creates some risk exposure for an institution. This guidance applies to links to affiliated, as well as non-affiliated, third parties. A link to a third-party website that provides a customer only with information usually does not create a significant risk exposure if the information being provided is relatively innocuous, for example, weather reports. Alternatively, if the linked third party is providing information or advice related to financial planning, investments, or other more substantial topics, the risks may be greater. Links to websites that enable the customer to interact with the third party, either by eliciting confidential information from the user or allowing the user to purchase a product or service, may expose the insured financial institution to more risk than those that do not have such features.

Reputation Risk

Customers may be confused about whether the financial institution or a third party is supplying the product, service, or other website content available through the link. The risk of customer confusion can be affected by a number of factors:

- nature of the third-party product or service;
- trade name of the third party; and
- website appearance.

Nature of Product or Service

When a financial institution provides links to third parties that sell financial products or services, or provide information relevant to these financial products and services, the risk is generally

[4] The Agencies' categories of risk include credit, market, liquidity, operational, legal, reputational, interest rate, price, foreign exchange, transaction, compliance, and strategic.

greater than if third parties sell non-financial products and services due to the greater potential for customer confusion. For example, a link from a financial institution's website to a mortgage bank may expose the financial institution to greater reputation risk than a link from the financial institution to an online clothing store.

The risk of customer confusion with respect to links to firms selling financial products is greater for two reasons. First, customers are more likely to assume that the linking financial institution is providing or endorsing financial products rather than non-financial products. Second, products and services from certain financial institutions often have special regulatory features and protections, such as federal deposit insurance for qualifying deposits. Customers may assume that these features and protections also apply to products that are acquired through links to third-party providers, particularly when the products are financial in nature.

When a financial institution links to a third party that is providing financial products or services, management should consider taking extra precautions to prevent customer confusion. For example, a financial institution linked to a third party that offers nondeposit investment products should take steps to prevent customer confusion specifically with respect to whether the institution or the third party is offering the products and services and whether the products and services are federally insured or guaranteed by the financial institution.

Financial institutions should recognize, even in the case of non-financial products and services, that customers may have expectations about an institution's due diligence and its selection of third parties to which the financial institution links its website. Should customers experience dissatisfaction as a result of poor quality products or services, or loss as a result of their transactions with those companies, they may consider the financial institution responsible for the perceived deficiencies of the seller.

Trade Names

If the third party has a name similar to that of the financial institution, there is an increased likelihood of confusion for the customer and increased exposure to reputation risk for the financial institution. For example, if customers access a similarly named broker from the financial institution's website, they may believe that the financial institution is providing the brokerage service or that the broker's products are federally insured.

Website Appearance

The use of frame technology and other similar technologies may confuse customers about which products and services the financial institution provides and which products and services third parties, including affiliates, provide. If frames are used, when customers link to a third-party website through the institution-provided link, the third-party webpages open within the institution's master webpage frame. For example, if a financial institution provides links to a discount broker and the discount broker's webpage opens within the institution's frame, the appearance of the financial institution's logo on the frame may give the impression that the financial institution is providing the brokerage service or that the two entities are affiliated. Customers may believe

that their funds are federally insured, creating potential reputation risk to the financial institution in the event the brokerage service should fail or the product loses value.

Compliance Risk

The *compliance risk* to an institution linking to a third-party's website depends on several factors. These factors include the nature of the products and services provided on the third-party's website, and the nature of the institution's business relationship with the third party. This is particularly true with respect to compensation arrangements for links. For example, a financial institution that receives payment for offering advertisement-related weblinks to a settlement service provider's website should carefully consider the prohibition against kickbacks, unearned fees, and compensated referrals under the Real Estate Settlement Procedures Act (RESPA).[5]

The financial institution has compliance risk as well as reputation risk if linked third parties offer less security and privacy protection than the financial institution. Third-party sites may have less secure encryption policies, or less stringent policies regarding the use and security of their customer's information. The customer may be comfortable with the financial institution's policies for privacy and security, but not with those of the linked third party. If the third-party's policies and procedures create security weaknesses or apply privacy standards that permit the third party to release confidential customer information, customers may blame the financial institution.[6]

B. RISK MANAGEMENT TECHNIQUES

Introduction

Management must effectively plan, implement, and monitor the financial institution's weblinking relationships. This includes situations in which the institution has a third-party service provider create, arrange, or manage its website. There are several methods of managing a financial institution's risk exposure from third-party weblinking relationships. The methods adopted to manage the risks of a particular link should be appropriate to the level of risk presented by that link as discussed in the prior section.[7]

---

[5] Section 8 of RESPA (12 USC 2607). The Department of Housing and Urban Development (HUD) issued a policy statement on June 7, 1996 entitled "Computer Loan Origination Systems" that addresses some issues that may arise in a weblinking arrangement. 61 Fed. Reg. 29,255. At this time, however, HUD has not provided guidance on how section 8 of RESPA applies to weblinking arrangements.

[6] Title V of the Gramm-Leach-Bliley Act (Pub. L. 106-102) and the agencies' implementing regulations (12 CFR Parts 40, 332, 573, and 716, hereinafter referred to as the "Privacy Regulations") govern the disclosure of nonpublic personal information by financial institutions to nonaffiliated third parties. The Agencies have also adopted the *Guidelines Establishing Standards for Safeguarding Customer Information* (12 CFR Parts 30, app. B; 364, app. B; 570, app. B; and 748, app. A).

[7] See *Risk Management of Outsourced Technology*, FFIEC, (November 28, 2000); http://www.ffiec.gov/exam/InfoBase/documents/02-ffi-risk_mang_outsourced_tech_services-001128.pdf

Planning Weblinking Relationships

In general, a financial institution planning the use of weblinks should review the types of products or services and the overall website content made available to its customers through the weblinks. Management should consider whether the links support the institution's overall strategic plan. Tools useful in planning weblinking relationships include:

- due diligence with respect to third parties to which the financial institution is considering links; and
- written agreements with significant third parties.

Due Diligence

A financial institution should conduct sufficient due diligence to determine whether it wishes to be associated with the quality of products, services, and overall content provided by third-party sites. A financial institution should consider more product-focused due diligence if the third parties are providing financial products, services, or other financial website content. In this case, customers may be more likely to assume the institution reviewed and approved such products and services. In addition to reviewing the linked third-party's financial statements and its customer service performance levels, a financial institution should consider a review of the privacy and security policies and procedures of the third party.[8] Also, the financial institution should consider the character of the linked party by considering its past compliance with laws and regulations and whether the linked advertisements might by viewed as deceptive advertising in violation of Section 5 of the Federal Trade Commission Act.

Agreements

If a financial institution receives compensation from a third party as the result of a weblink to the third-party's website, the financial institution should enter into a written agreement with that third party in order to mitigate certain risks. Financial institutions should consider that certain forms of business arrangements, such as joint ventures, can increase their risk. The financial institution should consider including contract provisions to indemnify itself against claims by:

- dissatisfied purchasers of third-party products or services;
- patent or trademark holders for infringement by the third party; and
- persons alleging the unauthorized release or compromise of their confidential information, as a result of the third-party's conduct.

The agreement should not include any provision obligating the financial institution to engage in activities inconsistent with the scope of its legally permissible activities. In addition, financial institutions should be mindful that various contract provisions, including compensation arrange-

[8] Useful information on the customer service performance of a potential linking party may be available in a number of ways. For example, the financial institution may ask the party directly for information on its level of customer complaints or it can check with organizations such as the Better Business Bureau or any functional regulator of the linking party.

ments, may subject the financial institution to laws and regulations applicable to insurance, securities, or real estate activities, such as RESPA, that establish broad consumer protections.

In addition, the agreement should include conditions for terminating the link. Third parties, whether they provide services directly to customers or are merely intermediaries, may enter into bankruptcy, liquidation, or reorganization during the period of the agreement. The quality of their products or services may decline, as may the effectiveness of their security or privacy policies. Also potentially just as harmful, the public may fear or assume such a decline will occur. The financial institution will limit its risks if it can terminate the agreement in the event the service provider fails to deliver service in a satisfactory manner.

Some weblinking agreements between a financial institution and a third party may involve ancillary or collateral information-sharing arrangements that require compliance with the Privacy Regulations.[9] For example, this may occur when a financial institution links to the website of an insurance company with which the financial institution shares customer information pursuant to a joint marketing agreement.

Implementing Weblinking Relationships

The strategy that financial institutions choose when implementing weblinking relationships should address ways to avoid customer confusion regarding linked third-party products and services. This includes disclaimers and disclosures to limit customer confusion and a customer service plan to address confusion when it occurs.

Disclaimers and Disclosures

Financial institutions should use clear and conspicuous webpage disclosures to explain their limited role and responsibility with respect to products and services offered through linked third-party websites. The level of detail of the disclosure and its prominence should be appropriate to the harm that may ensue from customer confusion inherent in a particular link. The institution might post a disclosure stating it does not provide, and is not responsible for, the product, service, or overall website content available at a third-party site. It might also advise the customer that its privacy polices do not apply to linked websites and that a viewer should consult the privacy disclosures on that site for further information. The conspicuous display of the disclosure, including its placement on the appropriate webpage, by effective use of size, color, and graphic treatment, will help ensure that the information is noticeable to customers. For example, if a financial institution places an otherwise conspicuous disclosure at the bottom of its webpage (requiring a customer to scroll down to read it) prominent visual cues that emphasize the information's importance should point the viewer to the disclosure.

[9] Under the Privacy Regulations, generally, financial institutions may not disclose non-public personal information about a customer to non-affiliated third parties without notifying the affected consumer about the disclosure and must provide him or her with an opportunity to exercise his or her opt-out right. However, there are certain exceptions to the notice and opt-out requirements, such as circumstances in which a financial institution discloses information in connection with the servicing or processing of a financial product that a consumer has requested (12 CFR §§ 40.14, 332.14, 573.14 and 716.14) and the disclosing of information to an unrelated financial institution under a "joint marketing agreement." (12 CFR §§ 40.13, 332.13, 573.13 and 716.13).

In addition, the technology used to provide disclosures is important. While many institutions may simply place a disclaimer notice on applicable webpages, some institutions use "pop-ups," or intermediate webpages called "speedbumps," to notify customers they are leaving the institution's website. For the reasons described below, financial institutions should use speedbumps rather than pop-ups if they choose to use this type of technology to deliver their online disclaimers.

A "pop up" is a screen generated by mobile code, for example Java or Active X, when the customer clicks on a particular hyperlink. Mobile code is used to send small programs to the user's browser. Frequently, those programs cause unsolicited messages to appear automatically on a user's screen. At times, the programs may be malicious, enabling harmful viruses or allowing unauthorized access to a user's personal information. Consequently, customers may reconfigure their browsers or install software to block disclosures delivered via mobile codes.

In contrast, an intermediate webpage, or "speedbump," alerts the customer to the transition to the third-party website. Like a pop-up, a speedbump is activated when the customer clicks on a particular weblink. However, use of a speedbump avoids the problems of pop-up technology, because the speedbump is not generated externally using mobile code, but is created within the institution's operating system and cannot be disabled by the customer.

Customer Service Complaints

Financial institutions should have plans to respond to customer complaints, including those regarding the appropriateness or quality of content, services, or products provided or the privacy and security policies of the third-party site. The plan also should address how the financial institution will address complaints regarding any failures of linked third parties to provide agreed upon products or services.

Monitoring Weblinking Relationships

The financial institution should consider monitoring the activities of linked third parties as a part of its risk management strategy. Monitoring policies and procedures should include periodic content review and testing to ensure that links function properly, and to verify that the levels of services provided by third parties are in accordance with contracts and agreements.[10] Website content is dynamic, and third parties may change the presentation or content of a website in a way that results in risk to the financial institution's reputation. Periodic review and testing will reduce this risk exposure. The frequency of review should be commensurate with the degree of risk presented by the linked site.

[10] In monitoring the customer service levels of linked parties, an institution can review its own records of customer complaints received regarding a particular party. The institution might also consider the other sources described in footnote 8 on due diligence.

Managing Service Providers

Financial institutions, especially smaller institutions, may choose to subcontract with a service provider to create, arrange, and manage their websites, including weblinks. The primary risks for these financial institutions are the same as for those institutions that arrange the links directly. However, if a financial institution uses a set of pre-established links to a large number of entities whose business policies or procedures may be unfamiliar, it may increase its risk exposure. This is particularly true in situations in which the institution claims in its published privacy policy that it maintains certain minimum information security standards at all times.

When a financial institution subcontracts weblinking arrangements to a service provider, the institution should conduct sufficient due diligence to ensure that the service provider is appropriately managing the risk exposure from other parties. Management should keep in mind that a vendor might establish links to third parties that are unacceptable to the financial institution. Finally, the written agreement should contain a regulatory requirements clause in which the service provider acknowledges that its linking activities must comply with all applicable consumer protection laws and regulations.

Financial institution management should consider weblinking agreements with its service provider to mitigate significant risks. These agreements should be clear and enforceable with descriptions of all obligations, liabilities, and recourse arrangements. These may include the institution's right to exclude from its site those links the financial institution considers unacceptable. Such contracts should include a termination clause, particularly if the contract does not include the ability to exclude websites. Finally, a financial institution should apply its link monitoring policies discussed above to links arranged by service providers or other vendors.