



OCC BULLETIN

Comptroller of the Currency
Administrator of National Banks

Subject: Weblinking

Description: Message to Bankers and Examiners

To: Chief Executive Officers of National Banks, Federal Branches and Agencies,
Service Providers and Software Vendors, Department and Division Heads, and
All Examining Personnel

PURPOSE

This bulletin highlights the risks and provides risk management guidance concerning banks' weblinking relationships with third parties.

KEY POINTS

Banks that form weblinking relationships with both affiliated and unaffiliated third parties should:

- Conduct sufficient due diligence on the third parties with which they form weblinking relationships with respect to their ability to provide service and their overall information security and privacy policies to minimize strategic and reputation risk.
- Negotiate formal contracts or agreements defining the rights and responsibilities of the bank and third parties with which the weblinking relationships are established to minimize transaction and reputation risk.
- Display appropriate disclosures on the bank's website to ensure that customers are not confused about which products and services are offered by the bank and which products and services are offered by third parties in weblinking relationships to minimize transaction and compliance risk.

| CONTENTS | PAGE |
|--|------|
| Background and Scope..... | 2 |
| Definitions..... | 3 |
| Risks | 3 |
| Reputation Risk..... | 4 |
| Transaction Risk..... | 5 |
| Compliance Risk..... | 5 |
| Strategic Risk..... | 6 |
| Risk Management | 7 |
| Planning the Hyperlink Strategy | 7 |
| Due Diligence..... | 7 |
| Agreements..... | 8 |
| Implementing the Hyperlink Strategy..... | 9 |
| Contingency Plans..... | 9 |
| Disclaimers and Disclosures..... | 9 |
| Monitoring the Hyperlink Strategy | 11 |
| Implementation..... | 12 |
| Responsible Office | 12 |

BACKGROUND AND SCOPE

A bank engaged in electronic banking may wish to expand its activities to offer various electronic commerce activities to its retail customers. A common activity for banks is to offer an Internet – or virtual – mall. In many cases, the bank will not provide the products and services itself, but instead will arrange with merchants and other vendors to provide weblinks from the bank’s website to the third party’s website where customers may obtain products and services. For smaller banks, a cost effective alternative may be a subcontracting arrangement with a vendor that provides a virtual mall that the bank may make available to its customers.

The OCC has addressed some of the risk management issues related to bank weblinking relationships in corporate licensing decisions and legal approvals. For example, the OCC has found that a national bank may, as part of the finder authority¹, establish links from the bank’s website allowing its retail customers to access third party, service provider websites.² These opinions the OCC has established

1 “A national bank may act as finder in bringing together a buyer and seller” which “includes, without limitation, identifying potential parties, making inquiries as to interest, introducing or arranging meetings of interested parties and otherwise bringing together parties together for a transaction that the parties themselves negotiate and consummate.” 12 CFR 7.1002.

2 See Conditional Approvals No. 221 (December 3, 1996) and No. 347 (January 29, 2000). National banks, in the exercise of their finder authority, may establish hyperlinks between their homepages and the Internet pages of third

the expectation that “banks will take reasonable steps to clearly distinguish between products and services that are offered by the bank and those offered by a third party or bank affiliate.”³ In addition, the OCC has concluded that weblinking arrangements between banks and third parties may provide for fees and other compensation to the bank. Under certain circumstances, banks may select such third parties based on their ability and willingness to provide favorable terms to the bank’s website customers.⁴

DEFINITIONS

A **weblinking** relationship with a third party involves both the bank’s website and the third party’s website. When a bank customer accesses a third party website from a bank’s website, the access is accomplished through a hyperlink.

A **webpage** is a viewable screen displaying information presented through a web browser in a single view sometimes requiring the user to scroll to review the entire page. A bank webpage may display the bank’s logo, provide information about bank products and services, or allow a customer to interact with the bank or third parties that have contracted with the bank.

A **website** consists of one or more webpages that may originate at one or more webserver computers. A person can view the pages of a website in any order, as he or she would a magazine.

A **hyperlink** is an electronic pathway that may be displayed in the form of highlighted text, graphics, or a button that connects one webpage with another webpage address.

RISKS

party providers so that bank customers will be able to access those nonbank webpages from the bank site. In addition, the OCC established that national banks may operate a “virtual mall,” i.e., a bank-hosted set of webpages with a collection of links to third party websites organized by product type and made available to bank customers for shopping. A range of financial and nonfinancial products and services are available via links to sites of third-party vendors. Merchants can confirm payment authorization electronically before shipping goods.

³ See Interpretive Letter No. 889 (April 24, 2000). In this letter, in permitting a bank to make a minority investment, the OCC stated that “...the bank should indicate that it does not provide, endorse or guarantee any of the products and services available through third-party webpages.”

⁴ Interpretive Rule 7.1002, 12 CFR.7.1002 provides that a national bank’s role as a finder includes, without limitation, identifying potential parties, making inquiries as to interest, introducing or arranging meetings of interested parties, and otherwise bringing parties together for a transaction. See Interpretive Letter No. 875, which describes a national bank’s role as “otherwise bringing parties together” which further provides that the bank may reasonably choose to bring together with its customers only merchants who are willing to provide a discount.

The primary risks to banks that provide direct access to third party websites for their customers through hyperlinks are those associated with their use of information technology: *reputation, transaction, compliance, and strategic*.⁵ The same risks exist for banks that subcontract with an intermediary third party (or parties) to arrange hyperlinks for their customers.

Reputation Risk

The performance of the third party and the website with which the bank links are major sources of *reputation* risk to the bank. Bank customers may have expectations about the third parties with which the bank chooses to link its website. Should customers experience disappointment, poor quality products or services, or loss as a result of their transactions with linked companies providing products and services, they may attempt to hold the bank responsible for the perceived deficiencies of the third party. Among other things, customers could assert that the hyperlink from the bank's site constitutes an implied endorsement of the third party or its products or services.⁶ If a bank subcontracts with a third party service provider to arrange the hyperlinks, the bank has *reputation* risk associated with the performance of the third party service provider that is arranging those hyperlinks.

The bank is also exposed to *reputation* risk with respect to the security and privacy policies and procedures of linked third party websites. The customer may be comfortable with the bank's policies on privacy and security, but not with those of the linked third party.⁷ If the third party, through security holes or privacy standards that are more lax than the bank's standards, allows the release of confidential customer information, customers may blame the bank.

Other sources of *reputation* risk to the bank are the technical and design standards of the third party website. System availability and other technical factors supporting the third party website contribute to the bank's *reputation* risk, because they affect the ability of the bank customer to access the linked sites. In addition, the format and content of the third party website may change over time in a way that is not acceptable to the bank and its customers. Links from third party websites to a bank website may also create a *reputation* risk exposure. These links, which are often referred to as *passive links*, may be part of a reciprocal agreement between the bank and a third party.

5 See OCC Bulletin 98-3, "Technology Risk Management," (February 4, 1998), and OCC Bulletin 98-38, "Technology Risk Management: PC Banking," (August 24, 1998).

6 Rockwell, Holly P., Annotation, "Products Liability Of Endorser, Trade Association, Certifier, or Similar Party Who Expresses Approval Of Product," 1 A.L.R. 5th 431 (1992); Kertz, Consuelo L. and Ohanian, Robbina, "Recent Trends in the Law of Endorsement Advertising: Infomercials, Celebrity Endorsers And Non-Traditional Defendants In Deceptive Advertising Cases," 19 Hofstra L. Rev. 603 (Spring 1991).

7 See Title V of the Gramm-Leach-Bliley Act (GLBA Pub. L. 106-10; 15 USC 6801, et seq.), its implementing regulation 12 CFR Part 40, and OCC Advisory Letter 99-6. Also see OCC Bulletin 2001-8, "Guidelines Establishing Standards for Safeguarding Customer Information," February 15, 2001.

Transaction Risk

The complexity of the information system underlying the bank's website and links to third party websites presents *transaction* risk. The more complex the system, the higher the *transaction* risk. The bank bears additional *transaction* risk if third parties offer less security and privacy protection than the bank to which it is linked. Third party sites may have less secure encryption policies, less stringent policies regarding the use of account numbers and passwords and weaker access controls than bank sites. Such differences present possible processing errors and potential legal actions creating *transaction* risk.

For the bank to benefit from a linking strategy, the links must function well technically. For links to function, the original software design must be sound and the website content must be well-maintained. The Internet service provider (the company that owns or controls the server that hosts the website), and the content providers (the bank and third party) all may have access to the link and the third party website. Access creates the possibility of errors and *transaction* risk exposure. If the bank subcontracts with an intermediary third party to arrange the hyperlinks for its customers, the complexity of the system increases the bank's exposure to *transaction* risk.

Compliance Risk

Compliance risk can arise from weblinking arrangements in a variety of ways, and the amount of compliance risk varies with the type of site to which a bank is linked. Fundamentally, because a bank's weblinking activity is based upon a national bank's finder authority (12 CFR 7.1002), the activity must be conducted consistent with the limitations of that authority.⁸ If the bank chooses to subcontract this finder function to a third party to establish weblinks for bank customers, the bank still bears the *compliance* risk exposure resulting from the third party finder arrangements.

A bank that operates a website with weblinks must comply with all consumer protection laws and regulations that apply to its operations. If the bank contracts with a third party to arrange for delivery of services, the arrangement must comply with applicable requirements. To the extent that a bank is engaged in the business of effecting transactions in securities for the account of others, the bank should consult applicable federal securities laws and regulations.⁹ In addition, some weblinking agreements

⁸ This does not apply to all links. National banks may enter into joint marketing relationships with third parties that relate to banking products and thus are not based on finder authority. Some of these joint relationships may involve both express bank endorsement and links from the bank's website to the joint party's site that would not be subject to limitations of 12 CFR 7.1002.

⁹ In particular, effective May 12, 2001, the blanket exemption from the definition of broker under the federal securities laws previously enjoyed by banks was changed to a more limited scope. Banks are only exempt from registration with the Securities and Exchange Commission (SEC) as a broker if their activities are excepted in 15 USC 78c(a)(4). Because of issues concerning the meaning of some of the new exemptions, the SEC has acted administratively to extend the effect of the prior broad exemptions until at least October 1, 2001.

between a bank and a third party may involve information-sharing arrangements that are regulated under Gramm-Leach-Bliley.¹⁰

The nature of the services or products provided by a third party may dictate what a bank's compliance obligations are. This is particularly true with respect to compensation arrangements. For example, a bank that is compensated for links to a third party that originates residential mortgage loans must consider the prohibitions against kickbacks and unearned fees under the Real Estate Settlement Procedures Act (RESPA).¹¹ 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.¹² Banks are subject to civil and criminal penalties for violating RESPA's anti-kickback and unearned fee prohibitions.

Strategic Risk

A *strategic* risk exposure is created if bank management fails to plan adequately for the implementation of hyperlinks on the bank website, either in-house or through service providers and software vendors. Part of the planning process will be selecting the appropriate third party relationships for the bank's hyperlink goals. The bank's goals will be based on its costs of supplying the links as well as on the needs and desires of the target population for the overall link strategy. An additional source of *strategic* risk is an inadequate contingency plan. A contingency plan should address failures of the third party servicer to provide agreed upon products and services, failures in the bank's or third party servicers' security controls, and remedies for inappropriate or unwanted weblinks.

10 Title V of the Gramm-Leach-Bliley Act and the OCC's implementing regulations (12 CFR Part 40) govern the disclosure of nonpublic personal information by banks to nonaffiliated third parties. Generally, banks may not disclose non-public personal information about a customer to 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 bank discloses information in connection with the servicing or processing of a financial product that a consumer has requested (12 CFR 40.14) and the disclosing of information to an unrelated financial institution under a "joint agreement" (12 CFR 40.13).

11 Section 8 of RESPA (12 USC 2607) prohibits a person from giving or accepting anything of value for referrals of settlement service business related to a federally related mortgage loan. It also prohibits a person from giving or accepting any part of a charge for services that are not performed. RESPA permits a payment to any person of a bona fide salary or compensation or other payment for goods or facilities actually furnished or for services actually performed. RESPA also permits affiliated business arrangements under which payments are made for goods furnished or services performed or as a return on an ownership interest or franchise relationship. However, certain disclosures concerning the relationship with the affiliate must be given, and the use of an affiliate generally may not be required. See 24 CFR 3500.15.

12 "Computer Loan Origination Systems" was published at 61 Fed. Reg. 29,255. At this time, HUD has not provided any time frame for any additional guidance it may issue concerning section 8 of RESPA and weblinking arrangements.

RISK MANAGEMENT

There are many methods of managing a bank's risk exposure from third party weblinking arrangements. Many of these methods are covered in the FFIEC's *Risk Management of Outsourced Technology Services*.¹³ However such risk is managed, the board or a board designee must effectively plan, implement, and supervise the monitoring of the bank's weblinking arrangement. As the bank plans its use of hyperlinks to provide access to third party websites, it should conduct sufficient due diligence to minimize its strategic risk and reputation risk. If the bank subcontracts these weblinking arrangements to an intermediary third party, the bank's due diligence responsibility applies to this third party as well as to firms to which the bank's customers will be linked. The bank's subcontracting agreement should have appropriate provisions to control risk. The bank is responsible for providing disclosures to consumers that are clearly written, prominently displayed and placed on the appropriate pages of a bank website to avoid customer confusion about which entity is supplying a product or service. A bank should also monitor selected hyperlinks to evaluate the effectiveness of the linking strategy and to determine whether the bank is referring its customers to websites that may pose security or privacy risks or that otherwise may fail to achieve customer satisfaction.

Planning the Hyperlink Strategy

Due Diligence

Because access to the third party is through the bank's website, customers are likely to associate the bank with the third party. To limit its reputation risk, bank management should conduct due diligence on third party products, services, or information provided to bank customers through hyperlinks. This consideration is especially important if the third parties are providing financial products, services, or information that customers may assume has been reviewed and approved by the bank. If the bank instead is contracting with a third party to arrange the hyperlinks, the bank should conduct sufficient due diligence on the third party service provider, to ensure that this third party is conducting appropriate due diligence on entities to which the bank's customers will ultimately link. Bank management should keep in mind that a vendor may establish links to third parties that are unacceptable to the bank.

Besides reviewing the third party's financials and its' customer service standards, a bank should review the privacy and security policies and procedures of the third party website. This review will help identify differences between the bank's standards and those of the third party servicer. It will also help to detect transaction and reputation risk exposures. If a customer is accustomed to dealing with the bank, which has historically provided a secure online environment, the customer may also "trust" the third party website. However, the third party may have poor security that may expose the customer to threats, such as data capture and fraud. In addition, if the third party's privacy policies differ from those of the bank, customers may not understand or accept that the bank does not control dissemination of information that customers provide at those sites. In either case, the customer may hold the bank

¹³ See FFIEC guidance "Risk Management of Outsourcing Technology," published as OCC Advisory Letter 2000-12, November 28, 2000.

responsible because the bank has provided the link.

During the due diligence process the bank should also review the presentation of the third party website to prevent bank customers from viewing offensive content. If the bank has contracted with a third party to select and maintain its weblinks, the bank should periodically review the linked websites for appropriate presentation and content.

Agreements

For banks that enter into weblinking agreements with third parties, the OCC expects understandable and enforceable definitions of all obligations, liabilities, and recourse arrangements. If an intermediary third party is able to add links to the bank's website, the bank should consider formally requiring that the service provider obtain the bank's authorization prior to introducing new links. In such agreements, the bank should reserve the right to exclude from its site links that the bank considers to be unacceptable. The bank should also include appropriate clauses that limit or preclude bank indemnification and that provide for appropriate information flows from third parties to the bank so that management has the ability to monitor activities going forward.¹⁴

Bank management should ensure that a bank's risk is limited when entering, maintaining, and ending the weblinking relationship. When entering the relationship, the agreements should specify that the parties are not forming a partnership or entering into a joint venture, regardless of the language used in marketing statements. In maintaining the relationship, bank management should consider two issues: the range of activities covered by the relationship and the compensation for these activities. The agreements should not obligate the bank to engage in activities that are inconsistent with the scope of permissible finder activities under 12 CFR 7.1002 or that are otherwise impermissible for the bank to conduct directly. In addition, management should review the compensation arrangements under these linking agreements. As finders, national banks are permitted to receive compensation for their linking arrangements with third parties. However, national banks should be mindful that compensation arrangements may invoke laws and regulations broader in scope than banking (ones that apply to all insurance and securities activities, for example, or ones, such as RESPA, that establish broad consumer protections).

Agreements with third parties should also cover conditions for ending or terminating the link. Third parties, whether intermediaries or firms providing services directly to customers, may go into bankruptcy, liquidation, or reorganization during the period of the agreement. The quality of their products or services, security, or privacy policies may decline; just as potentially harmful, the public may fear or perceive such a decline. The bank will limit its risk if these possibilities and their effects are addressed in the agreements.

¹⁴ *Ibid.* See footnote 4.

Banks may or may not form agreements concerning passive links with third parties. If bank management does form such agreements, including reciprocal linking rights, the OCC cautions that they should consider whether such links are in the bank's best interest.

Implementing Hyperlink Strategy

Banks must address a number of issues when they place hyperlinks to third parties on their websites. Bank management should develop contingency plans to cover a variety of situations that might arise. In addition, the strategy that banks choose when implementing linking should address customer confusion regarding linked third-party products and services that require time or other resources to resolve.

Contingency Plans

Banks should have contingency plans to cover a number of situations that might arise in weblinking arrangements with third parties. Contingency plans should address privacy and security issues that might arise between third parties and the bank. Although the bank's contracts and customer disclosures may address any policy differences in how third parties provide for the confidentiality and security of personal information, contingency plans should state how either party can change the way it implements these policies. The bank's contingency plan also should address how the bank will deal with any failures of third parties to provide agreed upon products or services. Such a failure might arise as a result of changes in management, cancellation of a product line, or a business failure of the third party. In addition, the contingency plan should address how bank management would handle inappropriate material on a linked third-party website.

Disclaimers and Disclosures

A bank can employ a variety of strategies in linking arrangements. For example, it could present a website that has the same look and feel throughout, regardless of whether the customer is viewing a bank webpage or that of a third party service provider. Alternatively, a bank could design webpages that provide links for its customers to bank products -- provided both by bank affiliates and by unrelated third parties. A bank could provide webpages that introduce customers to financial and nonfinancial products. All of these practices may confuse customers about which entity is offering the product, which increases the bank's risk. Providing adequate disclosures and disclaimers is important to mitigate this risk.

Effective disclosures should be written clearly and concisely. They should avoid communicating complicated information in a complex and technical way. Extensive or overly technical disclosures may simply add to a customer's confusion. Banks should clearly and conspicuously disclaim control or responsibility for the content, product, and services provided by linked sites.¹⁵ Banks should state

¹⁵ Some banks may use their website user agreement or customer agreement to disclaim responsibility for a third party's information, products, or services accessible through links. However, placing such disclosures in a user agreement is not a substitute for placing them more conspicuously as discussed above.

explicitly and conspicuously that they are not endorsing or guaranteeing the products, information, or recommendations provided by linked sites and that they are not liable for any failure of products or services advertised on those sites. In addition, bank management should inform consumers that each third party site may have a privacy policy different than that of the bank. Further, the bank should disclose that any of the linked third party websites may provide less security than the bank website.¹⁶ If the bank has contracted with a third party to arrange the hyperlinks for its webpage, the bank still has the responsibility to ensure that its customers receive the appropriate disclosures before linking with any third party service providers.

When designing the website disclaimer or disclosure, the bank should consider whether customers could be confused by the format or placement of the disclosure within the website as well as by the content. The bank should prominently display the disclosures on the website, ensuring that the disclosure's size, color, and graphic treatment makes it noticeable to bank customers.¹⁷ For example, if a bank places a disclosure at the bottom of its webpage, requiring a customer to scroll down to read it, obvious visual cues — ones that emphasize the information's importance — should point the reader to the disclosure. If there are several webpages that provide links to the same third party website, customer confusion may be minimized by using the same style for the hyperlinks.

Disclosures or disclaimers are especially important if a bank chooses to “frame” or otherwise heavily brand the webpages of linked third parties.¹⁸ If the bank's name or logo appears prominently on the webpages of third party websites, the bank risks confusing customers into believing that the bank could provide the site's financial products and services directly. For example, a bank that links to a discount broker with webpages that display the bank's logo may give the impression that the bank is providing the brokerage service, leaving customers confused about whether their deposits are federally insured.¹⁹

Some bank webpages may display links to bank products and services as well as links to nonbank products and services. If the nonbank products are financial in nature, disclosures alone will probably not eliminate customer confusion. In such circumstances, the bank should carefully delineate its

16 Refer to OCC Advisory Letter 99-6, “Guidance to National Banks on Web Site Privacy Statements.” For example, the bank may store customer transaction information in encrypted form only, but third parties with which the bank links may not be able to afford to do so.

17 “Advertising and Marketing on the Internet,” September 2000, Federal Trade Commission. If disclosures for specific third party products and services are overly long or complex, banks may consider establishing a separate webpage for more detailed explanations.

18 “Framing” is a software technique that would allow a bank to surround a third party's Web page with its own material, creating a “frame.”

19 In Interpretive Letter 889 (April 24, 2000), the OCC stated that “for links to pages that provide nondeposit investment products, the disclosures should alert customers to risks associated with these products, for example, by stating that the products are not insured by FDIC, are not a deposit, and may lose value.”

products and services from those of third parties, perhaps by using the bank's distinctive logo or another visual cue.²⁰ The bank may need to provide multiple disclaimers, depending on the types of products and services that link to the bank webpage. The bank should ensure that customers are able to connect each disclaimer or disclosure with the product or service it applies to.

Monitoring Hyperlink Strategy

The bank should monitor the impact of third party linking activities on the bank's safe and sound operations, just as it would the impact of any third party relationship. This concern about effective monitoring extends to banks that subcontract with an intermediary third party to arrange the weblinks for its website as well as to banks that create their own weblinking arrangements. If a bank elects to employ an intermediary third party service provider to establish the bank's hyperlinks, it must monitor the activity of the third party as well as the hyperlinks if it is to manage its strategic, transaction, compliance, and reputation risk.

In addition to standard practices, bank management should be aware of special considerations with respect to linked third parties. Policies and procedures should include provisions for periodically testing links to third parties to ensure they function properly. Testing may be particularly appropriate after the bank modifies any portion of its website. If the bank has a contract with a third party to establish the bank's hyperlinks, this third party will probably be responsible for periodic testing. Bank management should ensure that it has appropriate access to any third party policies and procedures related to testing and that it receives appropriate documentation when testing takes place.

Bank management should ensure that third parties to which they are linked continue to provide appropriate products and services to bank customers, presented on a website that does not use images or text which may prove offensive to bank customers. Website content is dynamic, and third parties may change the presentation or content of a website in such a way that it may present a reputation risk to the bank.

IMPLEMENTATION

Safety and soundness examiners as well as compliance and bank technology specialists will review a bank's weblinking activities. Generally, examiners will identify new weblinking activities at banks as part of ongoing supervision. Depending on the significance of such activities and the examiners' assessment of the risk management at the bank, examiners may want to conduct a special review of such activity, or include such a review in the next scheduled exam. A review of weblinking activities would require a review of the bank's website, vendor management policies, and the adequacies of disclosures and disclaimers for bank and nonbank products and services. Examiners should record significant concerns about the bank's weblinking risk in the bank's risk assessment, compliance rating, and Uniform Rating

²⁰ Such an approach will also simplify compliance with the restrictions on the placement of the FDIC logo and the official advertising statement under 12 CFR 328.

System for Information Security (URSIT) composite ratings.²¹

RESPONSIBLE OFFICE

Questions regarding this banking issuance should be directed to Clifford A. Wilke, Director, Bank Technology Division at (202) 874-5920 or via e-mail: clifford.wilke@occ.treas.gov.

Clifford A. Wilke
Director, Bank Technology Division

²¹ See OCC Bulletin 2001-17, "Uniform Rating for Information Security," April 6, 2001