

# Compliance Corner

FEDERAL RESERVE BANK OF PHILADELPHIA



## Regulatory Penalties for Violations of the Truth in Lending Act or Regulation Z

by Kenneth J. Benton, Consumer Regulations Specialist

This is the second article in a two-part series addressing a bank's potential liability for violating the Truth in Lending Act (TILA) or Regulation Z, TILA's implementing regulation. The first installment, which appeared in the fourth quarter 2006 issue of *Compliance Corner*, examined a bank's potential damages to its customers in a private lawsuit for violations of TILA or Regulation Z. This article reviews the circumstances in which a bank's regulator will order reimbursement to the bank's customers because of TILA violations.

The federal banking agencies—the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), the Office of Thrift Supervision, the National Credit Union Administration, and the Farm Credit Administration (collectively, the agencies)—periodically examine the banks they supervise to verify compliance with applicable federal consumer laws.

Regulation Z is one of the laws for which they verify compliance, and section 108 of TILA<sup>1</sup> provides the framework for the agencies' enforcement authority and the protocol they follow when determining whether a violation warrants reimbursement to the customer. Section

<sup>1</sup> 15 U.S.C. § 1607.

continued on page CC4



CC2

Addressing the Risk of Bank Phishing Scams

CC11

*Compliance Alert:* Deceptive Loan Solicitations Mentioning Community Reinvestment Act Program Cash Grants or Equity Disbursements

*Compliance Corner* is published quarterly and is distributed via *SRC Insights* to institutions supervised by the Federal Reserve Bank of Philadelphia. *SRC Insights* is available on the Federal Reserve Bank's website at [www.philadelphiafed.org](http://www.philadelphiafed.org). Suggestions, comments, and requests for back issues are welcome in writing, by telephone (215-574-3769), or by e-mail ([joanne.branigan@phil.frb.org](mailto:joanne.branigan@phil.frb.org)). Please address all correspondence to: Joanne Branigan, Federal Reserve Bank of Philadelphia, SRC - 7th Floor, Ten Independence Mall, Philadelphia, PA 19106-1574.

Editor ..... Joanne Branigan  
Associate Editor ..... Katrina Beck  
Designer ..... Dianne Hallowell

*The views expressed in this newsletter are those of the authors and are not necessarily those of this Reserve Bank or the Federal Reserve System.*



## Addressing the Risk of Bank Phishing Scams

by Kenneth J. Benton, *Consumer Regulations Specialist*

Phishing is the practice of deceiving Internet users into providing sensitive personal information, such as a social security number, bank account number, or pin number, by using e-mails and websites that impersonate a trustworthy institution with a legitimate need for the information. The information can be used by the phishers to commit identity theft or can be sold to identity thieves. Banks are a natural target for phishing fraud because most banks provide Internet banking, which allows identity thieves to use the information they fraudulently obtain to access the victims' assets through the Internet. This article discusses possible measures that banks can adopt to reduce the risk of phishing attacks.

Phishing has been growing at an alarming rate. In the one-year period between November 2005 and October 2006, the Anti-Phishing Working Group (APWG), an association of businesses and law enforcement officials working to combat phishing, received 402,590 reports of unique, active phishing sites. That represents a staggering 448 percent increase in unique phishing sites compared to the same period a year ago, during which APWG received 89,803 reports of unique, active sites. Similarly, the Gartner Group reported the results of a survey it conducted in November 2006, which showed that the number of Americans who received phishing e-mails increased from 57 million in 2004 to 109 million in 2006. Gartner estimated that the losses from these attacks have grown to \$2.8 billion, and that the average loss per victim has nearly quintupled from \$257 in 2005 to \$1,244 in 2006.<sup>1</sup>

Unsurprisingly, more than 90 percent of phishing attacks are on financial institutions. In January 2007, seven of the companies most frequently targeted for phishing attacks were banks, though the Gartner study indicated that phishing attacks on banks are declining.<sup>2</sup> A 2004 study by Gartner hints at the impact of phishing on banks. The study reported that two million bank customers had their checking accounts raided, with an average loss of \$1,200. Under section 205.6 of Regulation E, the Federal Reserve's implementing regulation for the Electronic Funds Transfer Act, most of the losses from a phishing scam are borne by the

---

<sup>1</sup> See <[www.gartner.com/it/page.jsp?id=498245](http://www.gartner.com/it/page.jsp?id=498245)>.

<sup>2</sup> See <[www.phistank.com/stats/2007/01/](http://www.phistank.com/stats/2007/01/)>.

bank rather than the customer, depending on when the customer notifies the bank of the unauthorized transaction. Gartner said that online banking fraud accounted for most of those losses. The Gartner study also discussed the secondary costs of phishing scams, including increased employee time responding to telephone inquiries from customers affected by a phishing scam.

In a typical case, the identity thieves send out mass e-mails to consumers purporting to be from a legitimate company with which the consumer might do business, such as a bank or a payment service like PayPal. The e-mail will typically ask the customer to verify account information using a pretext, such as "It has come to our attention that your PayPal Billing Information records are out of date. That requires you to update the Billing Information." Most phishing e-mails will also threaten that the consumer's account will be suspended or terminated if the account information is not verified promptly.

The e-mail will contain a hyperlink with a web address that appears to be a legitimate variation of the actual company's address. The link inside the e-mail will either appear similar to the web address of the legitimate company the phisher is impersonating or will appear to be the actual uniform resource locator (URL) of the company being spoofed. Most users assume that if a hyperlink appears as a URL (e.g., <https://www.bank.com>), the link will automatically take the user to that URL. In fact, the Internet's language for coding and displaying information (known as hypertext markup language, or HTML) does not require any relationship between the information displayed in a link and the underlying URL behind the information displayed.

The creation of a counterfeit website is a relatively simple matter. The website of a bank, consisting of text, graphics, and other information, is transmitted in its entirety when a user browses the company's website. An HTML editor can save all of the information transmitted, including the graphics, which can then be used to create a counterfeit site that appears



identical to the website of the bank being impersonated. Some phishing sites even display the actual graphics of the bank's website they are impersonating by linking directly to the graphics of the bank's website.

Regrettably, the variety, sophistication, and evolving nature of phishing scams do not lend themselves to a single magic bullet to prevent them from happening. Instead, the best solution is to employ a multi-tiered approach that banks and their customers can initiate.

**Multifactor authentication.** In October 2005, the Federal Financial Institutions Examination Council (FFIEC) issued guidance on authentication procedures for Internet banking.<sup>3</sup> Many banks use single-factor authentication for Internet banking (meaning verification based on only one factor, such as information the customer possesses, like a username and password). Multifactor authentication requires that two or more authentication factors be used to access an account. A second factor might be something the customer has, such as a token. A third factor might involve the use of biometrics, such as a fingerprint or eye scan.

continued on page CC8

---

<sup>3</sup> "Authentication in an Internet Banking Environment," FFIEC October 12, 2005, available online at <[www.ffiec.gov/pdf/authentication\\_guidance.pdf](http://www.ffiec.gov/pdf/authentication_guidance.pdf)>.

# Regulatory Penalties for Violations of the Truth in Lending Act or Regulation Z ...continued from page CC1

108 specifies that each agency must examine the financial institutions they supervise for compliance with TILA and Regulation Z, while authorizing the Federal Trade Commission (FTC) to enforce it for all other creditors.<sup>2</sup> It also specifies the circumstances under which the agencies must order the banks they supervise to reimburse their customers for TILA violations.

## Violations Triggering Reimbursement: Understated APR or Finance Charge

To implement section 108's requirements, the agencies published a "Joint Statement of Policy on the Administrative Enforcement of the Truth in Lending Act—Restitution" in 1980. It identifies the procedures the agencies follow for reimbursement and the type of violations that will trigger reimbursement. Because of subsequent amendments to TILA, the agencies revised the guidance (the revised policy statement) in 1998, which is the latest statement from the agencies on this issue.<sup>3</sup>

As section 108 requires, the revised policy statement states that the only TILA violations subject to reimbursement are an understated annual percentage rate (APR) or an understated finance charge. An understated APR or finance charge occurs when a creditor discloses an APR or finance charge in the TILA disclosure statement that is less than the actual APR or finance charge for the transaction.<sup>4</sup> For ex-

<sup>2</sup> The FTC does not conduct compliance examinations because of the large number of creditors subject to its oversight, but it does conduct investigations in response to consumer complaints.

<sup>3</sup> 63 Federal Register 47495 (Sept. 8, 1998).

ample, an APR is disclosed as 10 percent when it is actually 15 percent. Or a finance charge is disclosed as \$10,000 when it is actually \$13,000. The harm here is that the customer is being charged an interest rate or finance charge that is higher than what the creditor disclosed.<sup>5</sup>

An understated APR or finance charge will always require restitution to the customer if it falls into one of three categories of behavior: 1) a clear and consistent pattern or practice of violations, 2) gross negligence, or 3) a willful violation that was intended to mislead the person to whom the credit was extended. If none of these circumstances are present, the agencies still have the authority to order reimbursement for isolated violations of an understated APR or finance charge, but they are not required to do so.

Regulation Z contains tolerances for both open- and closed-end credit transactions that must be considered when determining whether an understated APR or finance charge requires restitution.

## Tolerances for Errors

Regulation Z contains tolerances for both open- and closed-end credit transactions that must be considered when determining whether an understated APR or finance charge requires restitution. A tolerance provides a small, permissible margin of error for disclosures within which the APR and finance charge are still considered accurate. For open-end transactions, the tolerance for the APR is one-eighth of a percent.<sup>6</sup> For example, if the actual APR on a home equity line

<sup>4</sup> The revised policy statement incorporates the tolerance provided in TILA and Regulation Z when determining whether a finance charge or APR is understated. The tolerance is discussed in more detail below.

<sup>5</sup> If a creditor *overstates* an APR or finance charge, no restitution is required because the actual APR or finance charge is less than what the creditor disclosed.

of credit is 10 percent, the creditor is not in violation for an understated APR if the disclosed APR is between 9.875 percent and 10 percent. For closed-end credit, the tolerance varies depending on whether the loan's amortization is less than 10 years or more than 10 years. If it is less than 10 years, an APR is accurate if it is within one-quarter of a percent. For loans with repayment greater than 10 years, the tolerance is either one-eighth of a percent for regular loans (in which the amount of the payment always remains the same) or one-quarter of a percent for irregular loans (in which the amount of the payment varies).

To determine the finance charge tolerance, section 108(e)(1) of TILA and the revised policy statement instruct regulators to convert the applicable APR tolerance for the credit transaction into a dollar equivalent for the finance charge. For example, if the amount financed on an open-end loan were \$100,000, the applicable APR tolerance of one-eighth would convert to a finance charge tolerance of \$125. Note, however, that the tolerances do not apply to violations that are willful and intended to deceive.

A special tolerance rule applies for closed-end credit secured by real estate or a dwelling: even if the understated APR exceeds the applicable tolerance for regular and irregular loans, the APR will be considered accurate if: (1) the finance charge is not understated by more than \$100 on loans made on or after September 30, 1995, or \$200 for loans made before that date, and (2) the APR is not understated by more than the dollar equivalent of the finance charge error, *and*

---

<sup>6</sup> 12 C.F.R. §226.14(a), which provides: "An annual percentage rate shall be considered accurate if it is not more than 1/8 of 1 percentage point above or below the annual percentage rate determined in accordance with this section."

the understated APR resulted from the understated finance charge that is still considered accurate.

The revised policy statement provides an example to help clarify the application of the tolerance: "consider a single-payment loan with a one-year maturity that is subject to a one-quarter of one percent APR tolerance. If the amount financed is \$5,000 and the finance charge is \$912.50, the actual APR will be 18.25 percent. The finance charge generated by an APR of 18 percent (applying the one-quarter of one percent APR tolerance to 18.25 percent) for that loan would be \$900. The difference between \$912.50 and \$900 produces a numerical finance charge tolerance of \$12.50. If the disclosed finance charge is not understated by more than \$12.50, reimbursement would not be ordered."

#### **Calculating Restitution**

After a banking agency determines that a bank has made a TILA error subject to restitution, the next question is how to calculate the amount the bank must

pay. Section 108 specifies that consumers are not obligated to pay amounts in excess of the disclosed APR or finance charge. However, when calculating restitution, the agencies always add the tolerance to the APR the creditor disclosed. For example, if the creditor disclosed the APR on an irregular mortgage transaction as 10 percent, when the actual APR was 14 percent, the regulator would treat the disclosed APR as 10.25 percent because of the tolerance. This reduces the amount of the reimbursement the creditor will have to pay by the amount of the tolerance.

Restitution can be very expensive when the number of violations is significant. For example, Provident National Bank entered into a \$300 million settlement with the OCC and the San Francisco District Attorney's Office in 2000 concerning, among other deceptive practices, its Regulation Z violation for failing to treat the processing fee for credit card applications

After a banking agency determines that a bank has made a TILA error subject to restitution, the next question is how to calculate the amount the bank must pay.

as a finance charge since it only charged that fee to customers approved for credit. This resulted in an understated finance charge and APR. And in 2004, the Board ordered Citigroup to pay a civil money penalty of \$70 million for violating Regulation B and the predatory lending restrictions of Regulation Z by making loans without regard to the borrower's ability to repay them.<sup>7</sup>

**Failing to disclose the APR or finance charge.** The revised policy statement also addresses the situation in which the creditor fails to disclose the APR or finance charge. If the APR is not disclosed, the interest rate specified in the promissory note is treated as the APR. If the note does not specify a rate, consumers do not have to pay an amount greater than the actual APR reduced by one-quarter of one percent for first lien mortgage transactions. For all other loans, the rate is reduced by one percent of the actual rate. If the creditor fails to disclose the finance charge, no adjustment is awarded.

**Obvious errors.** If an APR is disclosed correctly, but the disclosed finance charge is understated, or if the finance charge is disclosed correctly, but the disclosed APR is understated, the agencies will not require adjustment if the error involved a disclosed value that is 10 percent or less of what should have been disclosed.

**Methods of adjusting consumer accounts.** When a creditor must reimburse a customer, the revised policy statement allows creditors to select one of two methods for calculating the adjustment: the lump sum method or the lump sum/payment reduction method. Under the lump sum method, the creditor makes a cash payment equal to the total adjustment ordered by the regulator. Under the lump sum/payment re-

duction method, the total adjustment to the consumer is made in two stages: 1) a cash payment that fully adjusts the consumer's account up to the time of the cash payment and 2) a reduction of the remaining payment amounts on the loan.

**Period subject to reimbursement.** Another important issue for creditors facing restitution is the backward time period during which violations are subject to reimbursement. This is known as the "corrective action period" (CAP). Under the Joint Statement, the CAP for open-end credit transactions is the last two years preceding the current examination. For closed-end credit transactions, the CAP applies to transactions containing the violation that were consummated since the date of the immediately-preceding examination.<sup>8</sup> However, if the closed-end violation was willful and intended to mislead the consumer, adjustments must be made to all affected consumer transactions since July 1, 1969—TILA's effective date.

In addition, if an understated APR or finance charge arises out of a practice that was identified during the prior examination and was not corrected by the date of the current examination, loans consummated since the bank received written notice of the violation are subject to reimbursement. For loans that have terminated and have not been previously identified as having an understated APR or finance charge, reimbursement is not required if the loan consummated more than two years prior to the current examination.

**Agency discretion to not award restitution.** Section 108 authorizes the agencies to waive restitution,

---

<sup>7</sup> This penalty did not occur in the context of a compliance examination but during the Board's consideration of a CitiFinancial application to acquire European American Bank. The point is that violations of TILA and Regulation Z can be very costly. More information can be found at <[www.federalreserve.gov/boarddocs/press/Enforcement/2004/20040527/attachment.pdf](http://www.federalreserve.gov/boarddocs/press/Enforcement/2004/20040527/attachment.pdf)>.

---

<sup>8</sup> The term "immediately-preceding examination" is used in section 108. The agencies had originally defined it to refer to the last *compliance* examination. But as a result of two court decisions holding that examination means *any* type of bank examination [see *First Nat'l Bank of Council Bluffs, Iowa v. Office of the Comptroller of the Currency*, 956 F.2d 1456, 1463 (8th Cir.1992) and *Consolidated Bank, N.A. v. United States Department of the Treasury*, 118 F.3d 1461 (11th Cir. 1997)], the agencies revised the restitution policy to refer to the last examination of any kind. However, "examination" does not include a supervisory visit or an inspection. It also does not include an examination of an affiliate or subsidiary.

even though a violation occurred, if they determine that the disclosure error resulted from unique circumstances that involve a clearly technical and non-substantive disclosure violation that did not affect the information disclosed to the consumer or otherwise mislead the consumer. Statistics from the FDIC suggest that banks are unlikely to obtain a waiver under this provision. In 1997, the FDIC reported that it had received 63 requests for a waiver between 1991 and 1996, only one of which was approved. In that instance, the FDIC determined that Regulation Z was not, in fact, violated.<sup>9</sup>

#### **Safety and soundness exception.**

The agencies also have some discretion with reimbursement if requiring an immediate adjustment would adversely affect the safety and soundness of the creditor. In this situation, the agency can order partial adjustment or full adjustment over an extended period of time.

#### **Other Restitution Issues**

Following are other issues creditors should be aware of in order to avoid restitution.

**Inaccurate credit insurance disclosures.** The TILA disclosures that must be used when a credit transaction includes credit insurance have always been problematic for creditors. Section 226.4(a)(7) of Regulation Z requires that charges for credit life, accident, health, or loss-of-income insurance that are written in connection with a credit transaction are considered a finance charge unless the creditor complies with the three requirements of section 226.4(a)(7): 1) the creditor discloses that the insurance is optional, 2) the premium is disclosed, and 3) the customer signs or

initials a written request to receive it. If a creditor fails to comply with all three requirements, but nonetheless excludes the premiums for credit insurance from the calculation of the finance charges, its TILA disclosures will understate the APR and finance charge. If either the understated APR or finance charge exceeds the tolerance, the creditor will be ordered to reimburse the customer for the amount of the violation exceeding the tolerance, and the credit insurance will remain in effect for the remainder of its term. This violation has resulted in large penalties from regulators

or court settlements in private class actions. For example, in 1997, the FTC ordered the Money Tree to pay up to \$1.2 million in restitution because it failed to disclose that credit insurance was optional and therefore

should have treated the insurance premiums as a finance charge.

**Liability of assignee of a creditor.** If a creditor voluntarily assigns a credit transaction to another creditor, and a Regulation Z violation is apparent on the face of the Truth in Lending disclosure statement, the assignee is subject to regulatory penalties. But if the assignment is involuntary, the assignee is not subject to regulatory action.

#### **Conclusion**

The revised policy statement provides a roadmap for creditors so they can calculate how much their regulator will order them to reimburse customers for TILA violations involving an understated APR or finance charge. The potential for a large damage award when many customers are affected by a violation is a reminder of the importance of banks maintaining a stringent compliance program and a system of internal and external controls to verify that the program is working properly. □

The agencies also have some discretion with reimbursement if requiring an immediate adjustment would adversely affect the safety and soundness of the creditor.

<sup>9</sup> "Requests for Relief from Reimbursement under the Truth in Lending Act," FDIC, March 10, 1997, available online at <[www.fdic.gov/news/news/financial/1997/fil9719.html](http://www.fdic.gov/news/news/financial/1997/fil9719.html)>.

# Addressing the Risk of Bank Phishing Scams ...continued from page CC3

The guidance stated that “where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.” FFIEC further stated that single-factor authentication is inadequate for high-risk transactions involving access to customer information or the movement of funds. To clarify the guidance, FFIEC issued “Frequently Asked Questions” on August 15, 2006, that address many questions generated by the original guidance.<sup>4</sup>

Most Internet-based financial services use single-factor authentication, usually a password, for customers to access their accounts. If an institution relies only on single-factor authentication, transactions lack adequate protection for sensitive consumer information and funds. When a customer is tricked into disclosing a password, a thief could use the information to access the customer’s accounts and potentially transfer funds.

---

<sup>4</sup> “Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment,” FFIEC August 15, 2006.

While regulatory guidance, by definition, is not mandatory but merely suggestive, many banks are implementing multifactor authentication.<sup>5</sup> Multifactor authentication adds an additional level of security to the logon procedure. While multifactor authentication is still subject to phishing attacks, it makes phishing more difficult. For example, if the phishing site tricks a customer into providing a username and password, and the bank site also required a hardware token, it would be more difficult, though not impossible, to gain access since the phisher cannot obtain the token from the consumer through a phishing e-mail.<sup>6</sup>

By making it more difficult for phishers to attack a bank website, multilevel authentication also has a deterrent value. Phishers conducting surveillance of a bank’s website might conclude that it would be easier to target a bank with weaker security. It is analogous to the car thief who avoids cars known to have a high level of security and instead targets ones with little or no anti-theft technology.

**Education programs.** The success of phishing rests on the odds that a certain percentage of consumers will respond to deceptive e-mails. Because these scams are propagated through sophisticated social engineering tactics, technology alone cannot stop the problem. Educating bank customers about the existence of phishing schemes and steps that customers can take to minimize their risks are key elements in preventing phishing schemes.

---

<sup>5</sup> “As Deadline Nears, Banks Toughen Net Protections,” *Boston Globe*, December 29, 2006.

<sup>6</sup> In the summer of 2006, phishers defeated Citibank’s token authentication using the “man-in-the-middle” phishing attack. See “Phishers Beat Bank’s Two-Factor Authentication,” *TechWeb*, July 14, 2006. In a “man-in-the-middle” attack, the phisher lures the user into providing logon information at a spoofed site. The phisher then transmits that information to the actual site and transmits the legitimate site’s responses back to the user. The phisher is thus situated between the user and the legitimate site. The phisher in the middle is invisible to the user.



Banks should be proactive in educating their customers about ways to avoid phishing scams. Because phishing scams often target online banking customers, bank websites provide a good medium to communicate with them. Banks should remind their customers of safe practices to follow when using the Internet. Banks can then monitor the number of hits to the warning link to determine whether customers are reading them. If the hits are relatively low, because some customers do not always click on separate links on bank websites, banks could also incorporate the warnings into the logon procedure to ensure customers are receiving them.

Banks must walk a fine line with education because they want to inform their customers without alarming them. The information in educational warnings could result in some cus-

tomers avoiding online banking for fear of identity theft. Banks obviously do not want to scare their customers away from Internet banking, especially since it is less expensive for banks to conduct transactions on their websites than in branches with tellers. Each bank must determine the appropriate balance in preparing educational materials that inform customers of safe practices to follow without causing undue alarm.

Many banks believe that customer education is a key tool. Alecia Kontzen, director of e-commerce risk at Wachovia, relies heavily on consumer education to help prevent phishing attacks. Wachovia uses a rotating marketing campaign on Wachovia's website, which has received many hits. She also emphasizes employee training for responding to phishing reports from customers.<sup>7</sup> Some banks also include educational materials in customers' monthly statements and periodically conduct educational seminars.

---

<sup>7</sup> Michael Sisk, "A Phish Story," *US Banker*, February 2005.

## Educating bank customers about the existence of phishing schemes and steps that customers can take to minimize their risks are key elements in preventing phishing schemes.

**Other prevention techniques.** Banks can also be proactive in detecting phishing scams before they occur. Phishing scams are increasingly being executed from abroad. Therefore, since IP addresses reveal the country from which the user is accessing the Internet, banks should monitor customer IP addresses for unusual activity when they attempt to log onto the bank's website. For example, if a customer always banks from the same IP address in Texas, and one night the bank receives a wire transfer request for that account at 2:00 a.m. from an IP address in Korea, the

bank's systems could be programmed to suspend the account temporarily while the bank contacts the customer to verify the proposed transaction.

Some banks also hire third parties to monitor domain name registrations. Phishers will often

register a domain name with a slight variation of the URL of the bank they are attempting to spoof, hoping that the slight variation will deceive customers into thinking they are banking on the legitimate site. If a bank learns of the registration of a suspiciously similar name, it can reasonably infer that a phishing site is likely being developed and respond accordingly. Some third-party vendors also offer services in which automated Internet software applications, known as "Internet bots," search for websites similar to the bank's website.

Other initiatives companies can undertake to protect against phishing include employee education, computer security enhancements, e-mail filters to prevent phishing e-mails from reaching bank employees, and other practices that can help reduce the risk of phishing attacks.<sup>8</sup>

---

<sup>8</sup> See <[www.microsoft.com/mscorp/safety/technologies/antiphishing/guidance.msp](http://www.microsoft.com/mscorp/safety/technologies/antiphishing/guidance.msp)>.

Banks should also stay well-informed about new developments in phishing fraud because phishing scams tend to evolve over time as identity thieves attempt to adapt their practices to newer security measures. The APWG maintains a newswire with recent developments in phishing and offers other resources to help combat phishing.

**Anti-phishing toolbars and browsers.** One important customer initiative to combat phishing is anti-phishing toolbars and web browsers that can detect phishing websites and alert the user. Currently, about 12 different phishing toolbars are available.

Because consumers must load anti-phishing toolbars onto their home computers, an important issue for banks is how they can encourage their customers to install them. One option is for the bank to list information about toolbars on its website, with a link to download them.

The toolbars typically employ one of two different approaches to determining whether a user is visiting a phishing site. The first approach, known as blacklisting, compares the URL a consumer is browsing against an updated registry of known phishing sites. If the web address appears in the registry, the toolbar warns the user. Some toolbars also employ whitelisting, in which a URL is first checked against a list of legitimate websites. If the URL appears on the list of safe sites, the user is notified that the site has been verified. If the URL does not appear on the white list, the toolbar checks it against the blacklist. If the URL appears on the blacklist, the toolbar warns the user.

The second toolbar approach uses heuristics, in which a rule-based algorithm examines whether a website has suspicious characteristics common to phishing sites and alerts the user if it determines the site is a likely phishing site. For example, if a site has multiple

links to graphics on other Internet domains, particularly sites that are frequently impersonated like eBay and PayPal, the algorithm will conclude it is likely a phishing site.<sup>9</sup> Most of the graphics used on a website should be on the same domain as the website. Linking graphics to external websites on different domains is a sign of a phishing website. Some toolbars will also display the country hosting the website. If a consumer's bank is based in Johnstown, Pennsylvania, but the toolbar says the site is originating in Russia, that information will help alert the consumer that the webpage is likely a phishing site.

Another important issue is the difference in the effectiveness of toolbars. In a recent article, *Phishing Phish: An Evaluation of Anti-Phishing Toolbars*, researchers at the CyLab at Carnegie-Mellon University

evaluated the effectiveness of 10 toolbars in detecting phishing sites. The study found that three of them detected 75% of the phishing sites tested, while four detected less than 50% of the phishing sites. One toolbar, relying solely

on heuristics, had a high rate of detecting phishing sites, but also made a significant number of "false positives," in which a legitimate site was incorrectly flagged as a phishing site. Banks should consult with their IT and legal departments for the best way to address these issues.

Web browsers are also joining the effort to combat

**Banks should also stay well-informed about new developments in phishing fraud because phishing scams tend to evolve over time as identity thieves attempt to adapt their practices to newer security measures.**

---

<sup>9</sup> An Internet domain refers to the root portion of an Internet address. For example, in the URL <http://www.federalreserve.gov/DCCA/CRA/crate.cfm>, the domain is [federalreserve.gov](http://www.federalreserve.gov). Some phishing sites display the graphics of the site it is spoofing to make the site appear authentic. A legitimate site, such as [www.bankofamerica.com](http://www.bankofamerica.com), would have no reason to be displaying the graphics from another financial institution's website located on a different domain, so the practice of linking to graphics on another Internet domain is inherently suspicious.

phishing. The latest editions of the major Internet browsers have built-in anti-phishing filters. Some browsers use a blacklist by default. Others use heuristics in addition to a blacklist to detect phishing sites. Typically, if the browser detects a site that it believes to be a phishing site, it will alert the user.

The method a toolbar or browser employs to detect phishing sites is important because some identity thieves have already developed a response that significantly diminishes the effectiveness of the blacklist approach. In a new technique dubbed “Rockphish,” some phishers are continuously changing the web address of the phishing site through the use of “botnets.”<sup>10</sup> Because blacklists check a web address against a database of known phishing sites, a phishing site whose web address constantly changes renders the blacklist ineffective. As a result, some experts recommend that users employ toolbars and browsers that do not rely exclusively on blacklists but that also employ heuristics.

## Conclusion

Phishing attacks remain a significant concern for banks. While no single magic solution exists to prevent them from happening, and the attacks will continue to evolve, banks can employ a multitiered approach to reduce the risk of such attacks being successfully executed. This approach could include multifactor authentication, customer and employee education, web monitoring for suspicious activities, and encouraging customers to use an anti-phishing toolbar and/or browser. □

---

<sup>10</sup> A botnet refers to a network of computers that has been secretly hijacked by a malicious computer program. A hijacked computer will appear to be operating normally but can secretly be performing other activities. In the case of phishing, the botnet uses the hijacked computer to host a phishing site. The IP address of the hijacked computer then becomes the IP address of the phishing site. By continually moving the phishing site to other computers in the botnet network, the IP address constantly changes and eludes detection on a blacklist registry. For more information on botnets, see John Markoff, “Attack of the Zombie Computers Is Growing Threat,” *New York Times*, January 7, 2006.

## Compliance Alert: Deceptive Loan Solicitations Mentioning Community Reinvestment Act Program Cash Grants or Equity Disbursements

The Federal Reserve has received inquiries and complaints from homeowners who received direct-mail loan solicitations encouraging them to apply for a “Community Reinvestment Act (CRA) program” that entitles them to cash grants or equity disbursements. Some of these solicitations seem to imply that the Federal Reserve endorses or supports the solicitations.

These solicitations are deceptive for several reasons. First, the CRA does not entitle individuals or anyone else to grants or loans. Second, the Federal Reserve does not endorse or sponsor mortgage loan programs. Any loan solicitation that implies the Federal Reserve is endorsing a loan program is a red flag of deception. Consumers should be very suspicious of lenders or mortgage brokers making deceptive claims.

If banks receive inquiries from customers about this issue, they can instruct them to call the Federal Reserve’s CRA Assistance Line at (202) 872-7584 or to e-mail inquiries to [crahelp@frb.gov](mailto:crahelp@frb.gov). Banks can also direct customers to the online consumer pamphlet from the Federal Reserve, *Looking for the Best Mortgage: Shop, Compare, Negotiate*, which contains useful information about shopping for home loans and is available at: [www.federalreserve.gov/pubs/mortgage/mortb\\_1.htm](http://www.federalreserve.gov/pubs/mortgage/mortb_1.htm).



FEDERAL RESERVE BANK  
OF PHILADELPHIA

---

Supervision, Regulation and Credit Department  
Ten Independence Mall  
Philadelphia, PA 19106

[www.philadelphiafed.org](http://www.philadelphiafed.org)

## E-Mail Notification Service

Would you like to read *SRC Insights* and *Compliance Corner* on our website up to three weeks before they are mailed? Sign up for our e-mail notification service today at [www.philadelphiafed.org/phil\\_mailing\\_list/dsp\\_user\\_login.cfm](http://www.philadelphiafed.org/phil_mailing_list/dsp_user_login.cfm).