It seems that people are becomingly increasingly innovative and aggressive in finding ways to rob banks. Here are some of the scams our members have brought to our attention recently.

Our September 2008 Consumer Tips newsletter can help your customers avoid becoming a victim of one of these scams.

<table>
<thead>
<tr>
<th>Scam</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>10/27/08</td>
<td>Threatening Letters</td>
</tr>
<tr>
<td>5</td>
<td>10/20/08</td>
<td>Phone Scam</td>
</tr>
<tr>
<td>4</td>
<td>9/4/08</td>
<td>Lottery scam</td>
</tr>
<tr>
<td>3</td>
<td>8/20/08</td>
<td>Suspension of online banking service</td>
</tr>
<tr>
<td>2</td>
<td>8/19/08</td>
<td>Publisher's clearing house letter</td>
</tr>
<tr>
<td>1</td>
<td>8/15/08</td>
<td>Notification of compromised account</td>
</tr>
</tbody>
</table>

Scam 6  
October 27, 2008

The FBI is investigating a hoax whereby threatening letters were sent to Chase Bank, the FDIC and the OTS. More than 50 letters were mailed from Amarillo, and most contained a powdery substance which so far appears harmless.

The FBI is asking for help in solving this crime. [More information...]

Scam 5  
October 20, 2008

Here is an unedited warning from Attorney General Greg Abbott warning about telephone calls attempting to steal from an IBAT member bank's customers:

Texans should be aware that telephone calls purporting to originate from the Orange Savings Bank may actually be from identity thieves attempting to steal from bank customers.

Bank customers in the 409 area code have reported receiving automated telephone calls informing them that their account or credit card with Orange Savings Bank has been compromised. The Vidor and Orange-based bank’s customers are asked to call a number and provide their account information. Orange Savings Bank customers should not call the number. The individuals responsible for the call are attempting to obtain customers’ personal identifying information and bank account numbers.

To be clear, Texans must not respond to an unsolicited e-mail or telephone call seeking sensitive personal or financial information. Legitimate banks do not call or e-mail customers seeking this information. Texans should delete the e-mail or hang up the phone.

Orange Savings Bank customers who receive these unsolicited calls should report them to Phonebusters at (888) 495-8501, or the U.S. Secret Service Houston Field Office at (713) 868-2299.

[back to top]

Scam 4  
September 4, 2008

Visitors Center - Special Fraud Alerts
Shortly after arriving to work this morning we received our first call from a gentleman in Michigan regarding a letter he received congratulating him on his recent lottery winnings. He did not believe he had won any money but made the effort to call and notify us that a lottery scam was being perpetrated and the checks were being issued on an account at our bank. He had verified through the Internet that the check was written on a legitimate business and found our bank on the Internet, also.

Since this morning, we have received several other calls from individuals wanting to verify whether the lottery checks were legitimate. All checks have been for $4,950. The checks appear authentic and even the owners of the account think the signature looks correct. The perpetrators must have scanned an authentic check to make such a quality reproduction.

One of the callers said the envelope bears a Canadian postmark and another caller said the phone number appeared to be out of Montreal, Canada.

---

**Scam 3**  
**August 20, 2008**

Our customers are receiving an e-mail from our bank advising their online banking service has been suspended. To re-activate click on the link provided. That link takes them to an exact copy of our bank's bona fide web site which then gives them a link to re-activate online banking. You know the rest of the story. We have taken down our online banking until we can figure out how to avoid this type scam.

[back to top]

---

**Scam 2**  
**August 19, 2008**

We have experienced calls over the last couple of days where one of our customer's accounts is being used in a publisher's clearing house scam, being mailed out of Canada. We have received calls outside the Texas area. What can I do to alert people to this? Ironically, one of my employees received the same letter, but her check was drawn on a bank in New Jersey. Are you all hearing anything on this?

[back to top]

---

**Scam 1**  
**August 15, 2008**

An emerging issue is worthy of your serious attention. Several Texas community banks have recently been the target of a particularly disturbing scam. Here's how it has worked . . .

~ A community (generally rural, but urban areas have been victimized as well) was blanketed with "robo-calls", e-mails and text messages directing the recipients to call either a toll-free or local number because their account had supposedly been compromised. This has been described as "phishing on steroids" by one observer.

~ Customers calling the number(s) provided reached a phone customized with the bank name and a message appearing to be from that bank.

~ Customers were directed to enter their debit card number, expiration date and PIN.

~ Accounts were hit, primarily from ATMs in Europe.

~ This scheme has generally been initiated over the weekend, and the damage is done by the time the bank opens on Monday morning.

New technology has made it possible to "spoof" e-mails, phone numbers (caller ID's can be manipulated to display the bank's name) and calls can be forwarded anywhere in the world cheaply and easily.
We have contacted various regulatory authorities requesting their assistance in this matter, as well as the Secret Service, who has several of these scams under active investigation.

Banks should be particularly wary of this particular scam. While you no doubt have much more experience and expertise in this area than we do, some preliminary thoughts to guard against this (and similar) scams would include:

~ Alert your staff and appropriate third party vendors to be especially aware of suspicious activity, with special attention paid to out-of-country debit/ATM transactions.

~ Continue to educate your customers to never give PINs, account numbers or other sensitive information to anyone - even if it appears to be legitimate, they should be very cautious. Additionally, any unsolicited communication from a financial institution should alert a consumer to verify the information elsewhere prior to returning the call, e-mail or text message.

~ If you have reason to believe there is a scam operating in your area, please contact the Secret Service. The Lubbock office is quite aware of and involved with this situation, and can be reached at 806.472.7347. The Dallas office is also involved and is a good contact at 972.868.3200.

We are working with various parties to determine the appropriate next steps, and will no doubt keep you apprised. In the meantime, we felt it important to make you aware of this disturbing development, and will provide any additional information as it becomes available.

[back to top]