

# SafeTalk

Summer 2002

Loss Control newsletter of the ABA-sponsored insurance program underwritten by Progressive

## Combating Check Fraud

Check fraud continues to plague the banking industry. The ABA-sponsored insurance program has recently seen an increase in counterfeit check losses incurred by community banks throughout the country. Even with the best controls in place, bankers are almost defenseless against advances in technology that make counterfeit and altered checks virtually undetectable. Processing procedures alone can no longer protect the institution against check fraud; it is critical that employees be trained to look for suspicious activity and to report this activity as soon as it is detected.

In 2000, we published a white paper entitled *Policy, Training, Practice and Technology (PTPT): Your Arsenal Against Check Fraud*. We include in this issue of SafeTalk (Pg. 5) an excerpt from this paper and encourage our insureds to alert every member of their staff to the importance of awareness at the front line. If you would like a complete copy of the paper or additional copies to share with your management team, it can be downloaded from our website at [www.progressivebanks.com](http://www.progressivebanks.com) or requested from your local agent or a Progressive underwriter.

## Dishonesty at the TOP

Employee dishonesty remains the most serious exposure covered under the Financial Bond. Even with strong controls in place, we see significant claims arising from malicious activity by individuals within the organization. Typically, the perpetrator is a low-salaried individual who needs additional income to solve a short-term problem and the intent is to pay it back "as soon as..." Adequate internal controls usually identify misbehavior in a relatively short time period, though these cases can easily creep into six-figure losses quite quickly.

But what happens when the perpetrator is at the top of the organization? Over the past twelve months, the ABA-sponsored insurance program has seen some of our most serious claims arising from embezzlement by top management. In some cases, this activity has impaired capital to the extent that the bank has been forced to close. Most companies provide executive managers with a tremendous latitude and trust their judgement implicitly.

The perception is that such highly-respected and well-paid individuals would never betray the trust bestowed upon them by their colleagues and their community. The reality is that human nature does not always live up to our expectations.

continued...

### In This Issue...

Dishonesty at the Top .....	1
Follow-up: Internet Banking Intrusions .....	2
Special Report: Combating Check Fraud.....	3-5
What Every Teller Should Know.....	5
Alert: Fax Marketing, Teller Collusion Schemes .....	6
Internet Banking Liability: Explaining to Directors.....	7
ClaimsBeat.....	8
Make Sure You're Covered Against Check Fraud .....	8
Program News .....	9

So how do you prevent employee dishonesty at the management level?

- **Active Board involvement:** It is the duty and responsibility of the Directors to oversee management, and ultimately the responsibility lies at the Board level. Over-reliance and trust in the CEO and CFO to manage the affairs of the bank is an abrogation of this duty - yet far more common than we'd like to see among our banks. Board meetings should be more than just a report from management to the board. Examination, questioning and discussion of issues should be an integral part of any Board meeting and reflected in the Board minutes.
- **Questioning any suspicious activity:** Whether involving peers, subordinates or even the President of the bank, question and report any suspicious activity and encourage people at all levels to do so. More than once we have found the clerk or colleague that could see what was happening but was afraid to report it.

- **Board accessibility:** Fear of repercussions is probably the biggest deterrent to employees reporting suspicious activity, particularly involving those above them. Explain to employees the responsibility of the Board as an overseer of management, and open a pipeline to make the Board accessible to employees. The ability to anonymously report suspicious management activity will highly increase the likelihood of an employee doing so.

The bottom line is question, question, question any suspicious activity at any level. The higher the level of the employee, the more serious the potential implications. In almost every management dishonesty situation we have investigated, everyone is shocked because they had full trust in the individual - just as your community has in your management team.

We'd love to hear your suggestions on steps to take to curb management dishonesty. Please forward your stories to Judi Kovach at [jkovach@progressive.com](mailto:jkovach@progressive.com).

## Follow Up : Internet Banking Intrusions

In November, we notified our customers that Progressive had learned of intrusions into the systems of two major Internet banking service providers last summer. We have begun to receive notices of potential claims from insureds impacted by these intrusions. We have also since learned of subsequent intrusions.

For the most part, the hackers are not transferring funds at the time of the hacks. Rather, we are just now seeing malicious activity arising from the use of confidential information obtained during the hacks that occurred one year ago. Armed with the appropriate information, the hackers are ordering checks drawn on customers' accounts, altering PIN codes and creating counterfeit checks.

If your institution offers Internet banking services to your customers, please ensure that you are taking extra steps to identify any suspicious activity that may occur on customer accounts. This may impact not only Internet banking customers, but all bank customers.

If you are aware of any potential problems regarding unauthorized access to confidential information, seek counsel immediately and determine what customer notifications and other remedial steps may be appropriate.

Visit us at

[www.progressivebanks.com](http://www.progressivebanks.com)

Now more than ever, [progressivebanks.com](http://www.progressivebanks.com) can save you valuable time!

Download:  
Electronic Applications **New**  
Coverage Summaries  
Applications  
Specimen Policies  
SafeTalks  
SafeAlerts  
White Papers  
Topical Loss Control Articles

A recent survey revealed that our customers find it "extremely valuable" to be able to access these tools on our website. During 2002, we will be enhancing our website to provide more resources that we think you'll find valuable.

For any questions concerning the web site, please contact Kevin Elvington at 800-274-5222 or [kevin\\_elvington@progressive.com](mailto:kevin_elvington@progressive.com)

# Special Report: Combating Check Fraud

A counterfeit check ring in Georgia continues to expand its reach into surrounding states. The perpetrators recruit “down and out” individuals from homeless shelters by offering food, lodging, drugs and cash, then send these individuals into local banks to cash counterfeit checks drawn on the bank. In one instance, approximately 20 checks drawn on an active account were presented for payment at five different branches over the course of three days. There was nothing detectable about the fraudulent checks: the checks were perfectly crafted and in sequence; the maker’s signature appeared valid; the presenters held valid identification; and there was money in the account. An alert teller, in processing the transaction, went beyond the usual steps - in scanning the activity on the account, she noticed the unusual level of recent transactions and alerted her manager. Guards in the other branches were notified immediately, and were waiting when the next perpetrator tried to cash a check at another branch.

Being trained to take the extra steps to look at “the bigger picture” and feeling comfortable alerting a manager to potentially suspicious activity enabled this teller to curb a potentially severe loss to her institution. Make sure that your front line is not simply a line of processors, but part of an aware team that is responsible to protect the assets of your institution.

In 2000, we published a white paper, which can be found on our website, *Policy, Training, Practice and Technology (PTPT): Your Arsenal Against Check Fraud*. The following is an excerpt from this paper. If you would like a complete copy of the paper or additional copies to share with your management team, please contact your local agent or your Progressive underwriter.

## Teller Training

Two principles should be incorporated into a teller training program. First, all new tellers should be assigned a mentor, preferably a teller who has been with the bank for some time and is very familiar with policies and procedures. This person should not only help the new teller learn how to do things, but also explain why these are done in a particular manner. If tellers know why a particular policy or procedure is required, it will elevate them above the status of a simple check processor. It will also encourage them to think about the policies and procedures in place and make suggestions for improvement.

Second, all tellers should have a “go to person” – a very experienced individual who has decision-making authority. When a teller’s suspicions are raised, he/she should have someone to go to for advice and who will deal with a customer if the customer becomes angry or demanding. It should be emphasized to the tellers that taking suspicions to the “go to person” is encouraged. This helps foster an environment where all employees of the bank take responsibility for, and an interest in, detecting fraud and preventing losses.

### *Characteristics of a Good Check*

If tellers do not know the characteristics of a legitimate check, they will not be able to spot a bogus one. Some items that should be explained in the training process:

- Explain what the numbers and symbols in the MICR line represent.
- The bank address printed on the check should always correspond to the appropriate Federal Reserve District for that bank. The first two digits of the routing/transit number in the MICR line indicate the Federal Reserve District. For example, if the MICR line shows the Federal Reserve District as 04 (Cleveland), but the address for the bank listed on the check is Dallas, suspicions should be raised. Counterfeiters will often change the routing number for the Federal Reserve

District Office contained in the MICR line to delay the processing of the check and to enable access to the funds before the check is returned as a counterfeit.

- The check number contained in the MICR line should correspond to the check number in the upper right hand corner of the check.
- There are fractional routing numbers contained in the top right-hand corner of checks. The four-digit number on the bottom of the fraction corresponds to the Federal Reserve District number where the check was issued. This number should correspond with the Federal Reserve District number contained in the MICR line.
- Most checks contain a perforation on at least one side. Tellers should be instructed to look for perforated edges.
- The numerical dollar amount contained on the check should match the written dollar amount.
- The check should not be postdated or stale.

### *Other Common Warning Signs*

While this list is not exhaustive, some of the more common warning signs are:

- A check does not have an MICR line at the bottom.
- The MICR ink feels raised or appears shiny. Magnetic ink used in the printing of MICR lines is dull and produces images which are flat on the paper, rather than raised and/or shiny.
- The name and address of the drawee bank is typed rather than printed. Tellers should also check for spelling errors.
- No printed drawer name and address or a typed name and address.
- Checks containing indications of erasures, whiteout, alterations or eradications.
- Checks printed on slippery poor quality paper, which does not resemble legitimate stock paper.

- Colors that smeared when rubbed with a moist finger.
- Checks containing the word “void” anywhere on the check. Certain check stock will cause this word to appear when the check is reproduced on a copier.
- Checks which state on the back that they contain security features such as watermarks or micro-printing. If so, the teller should examine the check for those features.
- Checks that are marked “non-negotiable,” as are often used in promotional mailings. The teller that is not paying attention to the check, but is simply a check processor, can easily overlook this.
- The handwriting contained on the payee line is different from the handwriting on the remainder of the check.
- Something has been added to the check. For example, a check which was originally made payable to one payee may have been altered to make it a joint payee.
- A check payable to a corporation is either being deposited into an individual’s account or cashed.
- Third-party checks. The “go to person” should always be consulted prior to the teller cashing a third-party check. If the third-party check is deposited into an account with the institution, back room personnel should be notified to monitor activity on the account. Frequently, dishonest corporate bookkeepers will intercept checks payable to the corporation, forge the corporation’s endorsement, add their own endorsement and deposit the checks into their account. As they will use different tellers or ATMs for their deposits, it is critical that the back room be alerted to monitor activity on the account.

### ***Guidelines for Cashing Checks***

- If a teller does not know the customer, two forms of identification should be required, since falsified personal picture identification can easily be obtained (procedures for verifying proper identification will be addressed in depth under training for new account representatives.)
- Be wary of new customers performing split deposits (depositing a check and receiving a portion of the proceeds back in cash.) This is very typical of a fraud scheme.
- When cashing “on us” checks, verify that the account on which the check is drawn has sufficient funds and is not a dormant account or flagged for any other reason.
- Verify that there is not a stop payment order on the item.
- Be wary of individuals who attempt to distract while the check is being reviewed. Individuals that attempt to pass bad checks want the checks scrutinized as little as possible. If the person becomes demanding or unruly, the teller should seek assistance from the “go to person.” If the check is bad and the teller seeks help, the individual will most likely leave the bank.

Finally, if tellers have any suspicions whatsoever, further inquiry is necessary and the “go to person” should be consulted. Under Regulation CC, additional holds on an item are permitted if there are suspicions as to the validity of the item.

## **New Account Representative Training**

Banks are already familiar with the “know your customer” rule. To prevent fraud, new account reps must spend time with new customers who want to open an account. Much can be gained by generally observing a customer’s body language and his/her responses to questions. New account reps should be encouraged to engage prospective customers in conversation and to ask pertinent follow-up questions for clarification. Legitimate customers may well like the personal attention they are receiving in such an encounter. Criminals, however, want to open the new account as quickly as possible with few questions asked.

### ***Observing Customer Behavior***

New account reps should be trained to observe a new customer’s behavior and look for suspicious activity. New account reps should look for:

- Is the customer nervous, fidgety or defensive when responding to questions?
- Does the customer respond to questions in a vague or unresponsive manner?
- Is the customer unable or unwilling to provide positive identification or to complete answers to questions required in the new account application?
- Does the customer give suspicious reasons for not having proper identification on their person or for not knowing the answers to questions asked in the application?
- Does the customer live outside of the bank’s geographical area? If so, ask why the customer does not utilize an institution closer to home, and pay attention to whether the answer seems truthful.
- Does the customer promise to provide answers or required identification at a later date if the account can be opened now? Does the customer act in a manner designed to distract attention (for example, by becoming angry or indignant or simply changing the subject to avoid answering a probing question)?

If the new account rep observes any of the above behaviors, a red flag should go up. Additional follow-up may be necessary and certainly the “go to person” should be consulted.

### ***Authenticating Identification***

Two forms of personal identification should be required to open a new account. Acceptable forms of identification would include driver’s license, state identification card, passport, alien registration card, military or government identification card, credit card or certified copy of a birth certificate.

The state driver’s license or identification card should be required as primary identification. The other forms of identification are easily counterfeited or forged and should only be used for secondary forms of identification.

With respect to the primary form of identification, examine it carefully:

- Does the photograph reasonably resemble the person applying for the new account? At the very least, the new account rep. should verify that the race and sex match.
- Do the physical descriptions contained on the primary identification card match the applicant? Since some people appear either older or younger than their ages, a range of plus or minus ten (10) years should be considered.
- Compare the height listed on the identification card to the individual applying for the account. A range of plus or minus four (4) inches should be considered.
- Compare the weight listed on the identification card with the person applying for the account. A range of plus or minus thirty (30) pounds should be considered.
- Compare the hair and eye color using a range of light to dark.
- Compare the signature on the card to the signature on the application to ensure that they are at least reasonably similar?
- Verify that the identification card has not expired.
- Check for evidence of tampering such as open lamination, erasures or alterations.
- Verify that the particular state's official stamp or holographic emblem is present. If the bank services a multi-state area, the new account rep. should be trained on the characteristics of the driver's license and state ID for each particular state. It would also be very useful to provide new account reps with a book describing various forms of ID and illustrating their characteristics.

For corporate or other business accounts, a corporate resolution, certificate of incorporation and corporate tax return should be requested. If the account is a sole proprietorship or partnership, the required filings for the County Clerks Office should be requested as well as tax returns.

### ***The Application***

The new account reps should be trained that any suspicions regarding the above should be immediately taken to the "go to person." Follow-up questions will also be necessary. Again, a legitimate customer will understand the bank's concern. A criminal will most likely get up and leave.

The new account reps should be trained that the application must be completed in its entirety. Moreover, training should include an explanation of why certain questions are asked. This will aid the new account rep. in determining whether there is the potential for fraud. For example, if the applicant is 45 years of age but lists no prior banking history in the application, this is grounds for suspicion and further inquiry. Similarly, if the applicant gives a post office box for a mailing address in an area where post office boxes are uncommon, this is also grounds for suspicion and should be followed up.

The new account reps should also be trained to examine the application and compare it to the primary identification card. Does

the address on the application match the address on the identification card? Does the birth date on the application fail to match the birth date on the identification card? Are there misspellings (for example, is the applicant's name misspelled in the application when compared to the primary identification card)? Likewise, do the spellings in the address match between the identification card and the application?

Other suspicious items that may be noted on an application and should be followed up on are:

- Misspelling of the employer's name.
- The applicant claims to run a business out of the home but has no home telephone number.
- The applicant does not know the telephone number for the listed employer.
- The applicant gives a home phone number which contains an area code outside of the geographic area for the bank.

After the new applicant leaves, a policy should be in place and new account reps trained to verify as much information as possible contained in the application. The first source to turn to would be a verification service such as ChexSystems or TeleChek. Home telephone numbers as well as business numbers should be verified using telephone books, directory assistance, cross-directories or free web sites that provide such services. Additionally, if a large-sum check is used to open the account, the legitimacy of the check as well as the availability of the funds should be verified.

Finally, a thank-you letter should be sent to the new account holder. Not only is this a nice customer service touch, but it will also indicate a problem if the letter is returned.

Like tellers, new account reps can be a key line of defense against check fraud. Training in the above areas will ensure that they are.

## **What Every Teller Should Know:**

Calling a customer to confirm a transaction, for any reason, is not an imposition. Your customer will appreciate that you are looking out to protect his account.

Call the customer immediately if:

- A transaction is above a certain dollar amount (predetermined by management)
- A transaction is unusually high for a particular account
- An account balance is unusually high or low
- There is an unusually high level of activity on an account
- Anything about the transaction, the check or the individual presenting the transaction looks suspicious

# ALERT!

## Fax Marketing Results in Class Action Suit Against Bank

A community bank was named in a class action suit for violation of the Telephone Consumer Protection Act of 1992 (TCPA). The plaintiff is a mortgage broker who received a “mass fax” from a third party hired by the bank to distribute its marketing materials. The fax included the bank’s rate sheet.

According to the TCPA, it is a violation of federal law to distribute unsolicited advertisements by fax to anyone without prior express consent. A prior business relationship is considered consent, unless the recipient of the fax withdraws that consent.

These types of suits have become increasingly popular. This plaintiff’s law firm has successfully prosecuted this kind of suit before. The law provides a \$500 penalty for each violation, meaning each fax sent, and triple that amount if the violation is committed knowingly and willfully. Currently Congress is considering similar legislation to regulate unsolicited email advertising.

The FCC recorded 778 complaints nationwide between April and October 2001. To date, they have issued approximately 70 citations for possible violations of the TCPA, and has imposed fines in excess of \$1.5MM. The Dallas Cowboys settled a suit for \$1.73MM, far less than the potential fine of \$62.5MM for having sent 125,000 faxes. A Hooters restaurant in Georgia filed for bankruptcy protection after it was ordered to pay \$11.8MM for sending almost 8,000 faxes to 1,322 residents. As of March 1, 2002, there were 10 similar class actions pending in the United States.

## From the OCC: Organized Gang and Teller Collusion Schemes

The Office of the Comptroller of the Currency (OCC) has advised of fraud schemes involving organized gangs and newly hired bank tellers. Organized gangs are aggressively recruiting bank tellers to cash forged savings account withdrawals from customer accounts, and to cash stolen United States Treasury checks. Tellers are reportedly being paid several hundred dollars per transaction to assist in this fraud scheme.

Federal law enforcement officials have learned that organized gangs are using coercion and threats of bodily harm to persuade individuals to assist them in the fraud scheme. In some cases, tellers already employed by financial institutions are being recruited. More commonly, individuals are being encouraged by gang members to apply for teller positions at financial institutions for the sole purpose of providing access to the institution’s operating systems and customer access information. Typically, the gang member provides stolen information to the teller who keys the information into the bank’s automated systems so it will appear as if customer visited the teller window. The perpetrators are careful to keep amounts under supervisory approval limits. As a result, detection is delayed until the victimized customer reports the fraud.

Organized gang activity has become more sophisticated and the sphere of influence of some gangs has expanded geographically. Banks should exercise care and due diligence in their hiring practices, and periodically evaluate internal controls over the teller area. Banks should also file a “Suspicious Activity Report” (SAR), if the situation warrants.

Any information that you have concerning this matter, or any questions about OCC’s SAR requirements, should be brought to the attention of the OCC.

# Internet Banking Liability: Explaining it to your Directors

So just when you've convinced the Board of Directors that your Internet banking product is secure and does not put the institution at risk...how do you answer their questions regarding the need for this new insurance coverage without sounding like your selection of vendors and controls wasn't adequate on the front end?

As we are now seeing identity theft resulting from Internet banking intrusions that occurred last summer, our banks are recognizing that they shouldn't wait until their policies expire to request a proposal for Internet Banking Liability coverage. To lend some assistance, we offer you some frequently asked questions and answers. If you have any questions, please consult with your agent or your Progressive underwriter.

### ***Don't we use a prominent Internet banking vendor?***

We've selected a prominent Internet banking vendor - but vendors that host programs for multiple banks are the most attractive targets for hacker intrusions. There already have been multiple incidents of hackers breaking into the servers of prominent Internet banking vendors, resulting in transfer of funds, extortion attempts, and threats of publishing confidential information.

### ***Doesn't the vendor have a disaster recovery plan?***

A disaster recovery plan is designed for continuity of operation - when it comes to explaining to customers why their accounts were accessed, information was viewed or funds were transferred, a disaster recovery plan on the part of the vendor lends little protection against potential lawsuits.

### ***I thought we were covered under our current policies...***

Internet banking presents new exposures not currently covered under traditional insurance policies. Allegations of invasion of privacy, for example, are generally covered under the GL policy and therefore excluded under the D&O policy. Standard GL exclusions for "professional services" or "banking activities" will exclude coverage for allegations if they arise from Internet banking activities. The Internet Banking Liability Policy was designed specifically to address these gaps in coverage.

### ***If we use a third-party vendor for Internet banking - we don't have any liability issues...***

When an issue arises, it's the bank that the customer will look to for compensation. Be sure that any lawsuits involving Internet banking will name the bank the customer knows and has trusted. When suits arise, we won't want to have to incur the expense and headaches of suing the vendor to be compensated.

### ***Won't our vendor indemnify us for any problems?***

Our vendor promises to indemnify us for any loss related to their services (although most contracts actually hold the vendor harmless for vendor negligence, errors or omissions - read their contract carefully). But even if the vendor assumes responsibility, when there is an intrusion and the vendor has to "make whole" multiple - even hundreds of - banks, their limited capital may not go very far.

### ***Don't we have all the controls in place? Even the regulators approved our Internet banking program...***

Internet banking losses usually have nothing to do with any wrongdoing or omissions on the part of the bank. Even with the best security measures in place, banks are being hacked. We have controls in place to prevent robbery or embezzlement - but we still buy bond coverage "just in case".

### ***We don't have many Internet banking customers...***

If we or our vendor is hacked, it doesn't matter how many Internet banking customers we have. If a hacker can access confidential data, they likely have access to the data on every customer of the institution. All it takes is one customer to experience a loss. And with the worldwide access to our Internet banking site, the bank is open to issues of copyright infringement, libel, etc. from not only customers, but also from competitors or anyone that can access the site.

### ***Our website is simple -***

### ***no one can move money out of the bank....***

Even if the bank only has an informational website, links to local community resources or other third parties can provide a source of exposure (any allegations of negligence or wrong - doing on the part of the third party may be attributed to the bank that promoted the linked website). Even the simple use of email can present exposures to virus or allegations of libel, slander or copyright infringement.

# Claims *Beat*

## Recent Claims...

could this happen to you?

A safe deposit customer of a large savings bank was 6 months behind in paying monthly fees. After several notices, the bank removed the safe deposit box and its contents, which included no items of monetary value, but simply an envelope of photo negatives. When the customer ultimately contacted the bank several months later to pay for the box, the bank was unable to find the negatives. Claiming distress at having lost her valuable negatives, the customer demanded \$75,000 in settlement to avoid filing a lawsuit.



A community bank followed a course of conduct routinely allowing a 30 to 60 day delay in loan payments from a customer operating a retail business, in spite of loan documentation which permitted foreclosure after 31 days. In preparation for a pending merger, the bank sought to sanitize their loan portfolio by strictly enforcing the default provisions of their loan agreements. The bank initiated foreclosure proceedings and replevied the customer's merchandise, resulting in the customer going out of business. The customer counter-claimed and hired an expert who asserted that the business was worth \$8MM. The bank ended up settling the counterclaim for \$875,000 and spent \$231,000 in attorney's fees.



A long-term employee inquired about opportunities in another area of the bank and was encouraged to apply for a lateral position in that area in order to gain the necessary skills. The employee elected not to apply for the position and several months later, on very good terms with her employer, resigned to seek other opportunities. Within six months, the former employee sued the bank for discrimination in not offering her the position, despite the fact that she had not applied for it. The bank settled for \$45,000 after spending \$70,000 in defense costs.

An aggressive regional bank purchased a series of small banks in rural communities at a rapid pace to expand its reach in the state. For one of its branches, it paid a significant bonus to recruit the highly respected loan officer in the town, who had 18 years of tenure at the local community bank. The loan officer had little supervision as his direct supervisor was in a city 30 miles away. In the course of an internal audit, a teller mentioned to the auditor that she thought it curious that she had never seen one of the officer's loan customers. The auditor subsequently pulled the loan and credit files for the customer, and when he drove out to the address listed for the customer, found that the address didn't exist. Further investigation revealed that the social security number was also falsified and that the customer's statements - as well as those of other "customers'" statements - were being sent to a post office box in the loan officer's name. The total loss to the bank is estimated at close to \$1MM in falsified loans.



A bank's customer bought and sold used cars. Based on the nature of the business, the bank president continually approved large overdrafts, which would be covered by the customer within 24 hours. Within 22 months, it was discovered that the customer and two other car dealers had operated a high-volume check-kiting scheme involving the bank and at least two other banks. The loss to the bank was over \$3.5MM.

## Make sure you're covered against Counterfeit Check fraud

Counterfeit checks are the most common tools for check fraud today and almost impossible to detect. Many bankers, however, are not aware that loss arising from the acceptance of counterfeit checks is not covered under the Financial Institution Bond. Bankers also are surprised to be caught uninsured when an unauthorized party endorses a check to embezzle funds. Unauthorized signatures are also not forgeries and losses due to acceptance of unauthorized signatures are not covered under the Bond.

Insuring Agreement D of the standard Financial Institution Bond provides the bank coverage for losses resulting from forgery or alteration of negotiable instruments. This agreement does not provide coverage for loss arising from the acceptance of counterfeited documents containing forgery, nor does it provide coverage for loss arising from the acceptance of an unauthorized signature on any instrument

*The availability of the Counterfeit Check Rider and Unauthorized Signature Rider over the past few years has been an important source of protection against check fraud in today's technologically-advanced society. To confirm that you have these important coverages on your Bond, check with your agent or with your Progressive underwriter.*

# Program News...

## Did You receive your Distribution Check?

Once again, in 2002, customers who are ABA members share in the distribution of \$4,000,000. If your bank was an insured of our program on January 15, 2002 and an ABA member in good standing you should have received a distribution check from our mutual reinsurer, ABPFIC. If you have not received your check, please check with your agent or your underwriter.

Many of our customers who were not previously ABA members have joined the ABA, as the distribution check they receive covers their ABA dues. To find out more about ABA membership call 1-800 BANKERS.

## Thanks For A Great Year!

We are happy to announce that 2001 was a milestone year for the ABA-sponsored insurance program - our largest year ever with over \$37,000,000 in premium written! We added 184 new customers to the program. The ABA-sponsored insurance program now serves over 1,600 financial institutions in all 50 states, and is endorsed by 26 state bankers associations.

*We appreciate your support and thank you for your business.*

## Internet Banking Liability Product Now available in 47 States\*

Our Internet Banking Liability product is receiving increased attention in the media and throughout the banking community as bankers better understand the exposures faced by online offerings. If you are offering, or considering offering, online banking and have not yet spoken with your agent or underwriter, call today to find out how to protect your institution against the risks of Internet banking.

\*coverage not available in LA, NY, MN, PR

## Case Studies in Risk Management: Internet Banking

In an effort to educate our insureds about the potential liability exposures presented by recent Internet banking intrusions, the ABA-sponsored insurance program has published a new loss control tool, Case Studies in Risk Management: Internet Banking. This publication was sent to all customers or their agents in March. If you have not received a copy or would like additional copies to share with your management team, please contact your local agent or your Progressive underwriter.

## New Tools You Can Use!

### Did you know that...

- our website, [www.progressivebanks.com](http://www.progressivebanks.com), now includes a wealth of program information, as well as the 2000 ABA Bank Insurance Survey (providing average limits purchased by financial institutions by peer group)?
- you can print applications, specimen policies and endorsements, coverage summaries, and loss control articles from our website?
- we are now emailing proposals, along with the supporting documents?
- we now have Electronic Applications which allow you to complete applications on your computer and send them electronically?

We are excited about using new technology to facilitate our processes for you. If you have any suggestions to improve our processes further, please let us know.

## Simplifying the Application Process...

### New Electronic Applications

It seemed inefficient in this world of computers to ask you to complete paper applications - so the ABA-sponsored insurance program is now making available **Electronic Applications**.

**Electronic Applications** are Microsoft Word documents that you can complete on your PC, save, print and email back to us or your agent. You will need to print, sign and send a hard copy of the application to bind coverage; but the rest of the process can be handled electronically. Plus, you'll be able to keep the file on hand and simply update when renewal time comes around.

**Electronic Applications** are now available on our website, or call your agent or underwriter. They'll be happy to email them to you.