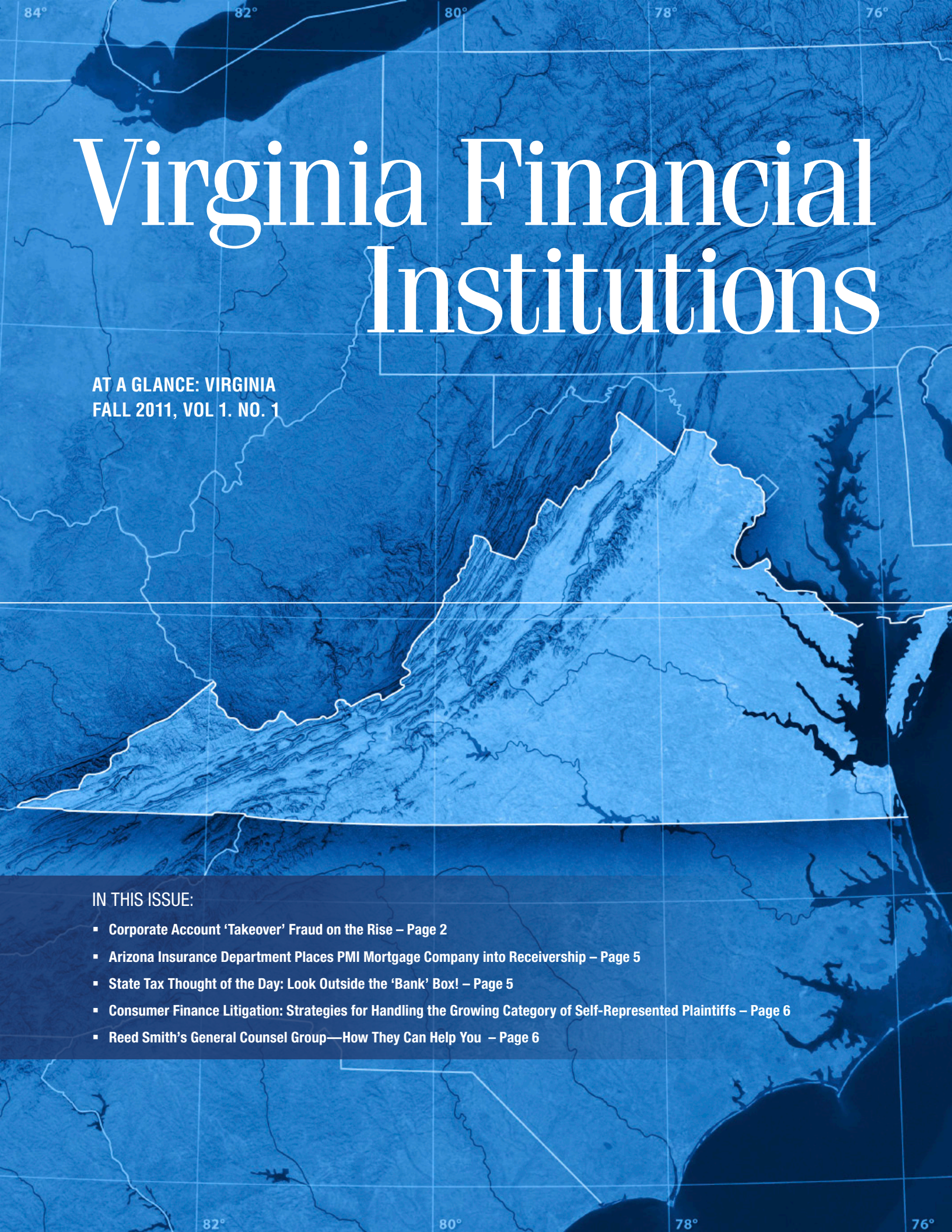


Virginia Financial Institutions

AT A GLANCE: VIRGINIA
FALL 2011, VOL 1. NO. 1

IN THIS ISSUE:

- Corporate Account 'Takeover' Fraud on the Rise – Page 2
- Arizona Insurance Department Places PMI Mortgage Company into Receivership – Page 5
- State Tax Thought of the Day: Look Outside the 'Bank' Box! – Page 5
- Consumer Finance Litigation: Strategies for Handling the Growing Category of Self-Represented Plaintiffs – Page 6
- Reed Smith's General Counsel Group—How They Can Help You – Page 6

CORPORATE ACCOUNT 'TAKEOVER' FRAUD ON THE RISE

Summary

Cyber criminals have developed ever more sophisticated and malicious techniques to perpetrate corporate account "takeovers" and transfer funds to criminal accounts overseas. Reported losses to businesses and financial institutions are in the hundreds of millions of dollars.

In response to this growing and evolving threat, the Federal Financial Institutions Examination Council recently issued supplementary guidance to its 2005 Guidance entitled *Authentication in an Internet Banking Environment*. The supplementary guidance requires depository institutions to adopt "layered security" and other authentication controls. Depository institutions may be examined for compliance with these new standards effective January 1, 2012.

Importantly, the supplementary guidance would appear to create a new standard of care by which an institution's actions will be examined in the event of litigation resulting from cyber fraud losses. The supplementary guidance and recent court cases indicate that financial institutions should review and update their authentication procedures and Internet banking forms.

Joseph ("Jay") E. Spruill, III
Counsel– Richmond, VA
Financial Industry Group
jspruill@reedsmith.com

Cyber Fraud Landscape

Financial institutions and businesses face a growing threat from cyber criminals who are using ever more sophisticated and malicious techniques to perpetrate deposit account "takeovers" and transfer funds, often to criminal accounts maintained overseas. In testimony before a subcommittee of the House Financial Services Committee in September, the Assistant Director of the FBI's Cyber Division said the FBI is currently investigating more than 400 reported cases of corporate account takeovers involving in excess of $255 million in attempted theft and approximately $85 million in actual losses. [1] He noted that in many cases, companies victimized by corporate account takeovers choose not to disclose their losses, so what the total amount of losses to industry and the economy might be is uncertain. What is certain is that this is a growing and evolving threat to the finances and reputations of businesses and financial institutions.

Importantly, this kind of fraud exploits financial system users, not the financial system itself. In this regard, small businesses are particularly vulnerable. In testimony before the Senate Banking Committee this summer, an expert indicated that a study he conducted found that 70 percent of small businesses did not have even basic security controls, such as firewalls, antivirus software, strong passwords, or basic security awareness for staff. [2] Weak security makes it easier for cyber thieves to penetrate a bank customer's computer system, obtain bank account login credentials, and initiate fraudulent electronic funds transfers from the account. Most cyber attacks of this kind target business accounts because of their high balances (providing more money to steal) and greater account activity (making it easier for the fraud scheme to succeed).

In response to the increasing threat, and concerns that customer authentication methods and controls at financial institutions have become less effective, the Federal Financial Institutions Examination Council ("FFIEC") issued new guidance this summer to supplement its 2005 Guidance entitled *Authentication in an Internet Banking Environment* ("2005 Guidance"). As discussed below, the recent guidance ("2011 Guidance") provides for tighter authentication standards for depository institutions to follow in managing their online banking operations. The 2011 Guidance becomes effective January 1, 2012. Institutions should take steps to modify their procedures and Internet banking forms in response to the 2011 Guidance by the end of the year.

Given the large sums of money lost in these attacks, it is not surprising that victims are increasingly suing their financial institutions to try to recover their losses. In particular, businesses that have suffered losses at the hands of cyber criminals have sought to hold their financial institutions liable for failing to detect and prevent the unauthorized withdrawal of funds from their accounts. Importantly, the 2011 Guidance would appear to create a new standard of care by which financial institutions' actions will be measured. Financial institutions should expect litigation in this area to increase and take steps to avoid potential liability. The current case law is examined below.

2011 Guidance: Expectations and Implications

In issuing the 2011 Guidance, the FFIEC indicated that there have been significant changes in the threat landscape and that cyber crime complaints have risen dramatically each year since 2005, particularly with respect to commercial accounts. The 2011 Guidance states:

Rapidly growing organized criminal groups have become more specialized in financial fraud and have been successful in compromising an array of controls. Various complicated types of attack tools have been developed and automated into downloadable kits, increasing availability and permitting their use by less experienced fraudsters. Rootkit-based malware surreptitiously installed on a personal computer (PC) can monitor a customer's activities and facilitate the theft and misuse of their login credentials. Such malware can compromise some of the most robust online authentication techniques, including some forms of multi-factor authentication.

The 2011 Guidance seeks to respond to the new threat by requiring financial institutions to review and update their existing risk assessments (i) as new information becomes available, (ii) prior to implementing new electronic financial services, or (iii) at least every 12 months. Updated risk assessments should consider, but not be limited to, the following factors:

- Changes in the internal and external threat environment
- Changes in the customer base adopting electronic banking
- Changes in customer functionality offered through electronic banking
- Actual incidents of security breaches, identity theft, or fraud experienced by the institution or industry

(continued)

The 2011 Guidance states that online business transactions involve a higher degree of risk because of the frequency and higher dollar amounts of these transactions.

Most importantly, the 2011 Guidance states that financial institutions should implement "layered security" utilizing controls consistent with the increased level of risk for business transactions. "Layered security" involves the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated by the strength of a different control. The 2011 Guidance provides that effective controls that may be included in a layered security program include, but are not limited to, the following:

- Fraud detection and monitoring systems that include consideration of customer history and behavior, and enable a timely and effective institution response
- The use of dual customer authorization through different access devices
- The use of out-of-band verification for transactions
- The use of "positive pay," debit blocks, and other techniques to appropriately limit the transactional use of the account
- Enhanced controls over account activities, such as transaction value thresholds, payment recipients, number of transactions allowed per day, and allowable payment windows (e.g., days and times)
- Internet protocol (IP) reputation-based tools to block connection to banking servers from IP addresses known or suspected to be associated with fraudulent activities
- Policies and practices for addressing customer devices identified as potentially compromised and customers who may be facilitating fraud
- Enhanced control over changes to account maintenance activities performed by customers either online or through customer service channels
- Enhanced customer education to increase awareness of the fraud risk and effective techniques customers can use to mitigate the risk

The 2011 Guidance provides that an institution's layered security program should contain, at a minimum, (i) manual or automated transaction monitoring or anomaly detection and response processes to detect and respond to suspicious account activity; and (ii) enhanced controls for customers and system administrators who are granted privileges to set up or change system configurations, such as setting access privileges and application configurations and/or limitations.

The 2011 Guidance also recommends that institutions offer multifactor authentication to their business customers. Such multifactor authentication may include device authentication or challenge questions. Importantly, the FFIEC agencies have concluded that simple device authentication, such as the use of cookies loaded onto a customer's PC to confirm it is the same PC that was enrolled by the customer, is no longer effective. Rather, institutions should use a more sophisticated form of technique that uses "one-time" cookies and creates a more complex digital "fingerprint" by looking at a number of characteristics, including PC configuration, Internet protocol address, geo-location, and other factors.

With respect to challenge questions, the 2011 Guidance provides that in view of the amount of information about people that is readily available on the Internet, and the information individuals make available about themselves on social networking websites, institutions should no longer consider basic challenge questions (e.g., mother's maiden name), as a primary control, to be effective. Rather, challenge questions should be sophisticated questions or "out-of-wallet" questions that do not rely on information that is publicly available.

Finally, the 2011 Guidance says a financial institution's customer awareness and educational efforts should be directed to both retail and commercial account holders, and include the following minimum elements:

- An explanation of protections provided, and not provided, to account holders relative to electronic funds transfers under Regulation E, and a related explanation of the applicability of Regulation E to the types of accounts with Internet access
- An explanation of under what, if any, circumstances and through what means the institution may contact a customer on an unsolicited basis and request the customer's provision of electronic banking credentials
- A suggestion that commercial online banking customers perform a related risk assessment and controls-evaluation periodically
- A listing of alternative risk control mechanisms that customers may consider implementing to mitigate their own risk, or alternatively, a listing of available resources where such information can be found
- A listing of institutional contacts for customers' discretionary use in the event they notice suspicious account activity or experience customer information security-related events

New Standard of Care

Importantly, the 2011 Guidance would appear to create a new standard of care against which a financial institution's actions will be measured in litigation involving cyber fraud losses. In the past, courts have looked to the 2005 Guidance in determining whether a financial institution adopted commercially reasonable methods of providing security against online fraud. In one case where a bank apparently delayed in complying with the 2005 Guidance, the court held that a reasonable finder of fact could conclude that the bank breached its duty to protect its customer's account against fraudulent access.[3] In another case, the court used the 2005 Guidance as a “yardstick” for measuring the commercial reasonableness of a bank’s authentication system.[4] Going forward, financial institutions should expect courts to use the 2011 Guidance in much the same way.

Recent Cases

Two recent court decisions address the issue of a bank’s liability for the unauthorized withdrawal of funds from a corporate deposit account resulting

(continued)

from cyber fraud. In one case, a federal district court in Michigan ruled that the bank was liable because it had acted in "bad faith" in failing to prevent the unauthorized withdrawals. In the other, a federal district court in Maine held that the bank was not liable because the customer had agreed to a commercially reasonable security procedure used by the bank, despite the fact that such procedure did not prevent the fraud.

In *Experi-Metal, Inc. v. Comerica Bank,*[5] a company's controller was duped by a phishing scheme. The controller was sent an email, purportedly from the company's bank, directing him to a web page where he was asked to provide account information. Believing the email to be a legitimate request from the bank, the controller complied and entered his company's confidential customer identification, password, and secure token number. Within hours of this criminal hijacking of the account, more than $1.9 million had been transferred from the account to destinations around the world. The bank was able to get much of this amount back, but $560,000 was never recovered. The company sued the bank for this amount.

As an initial matter, the court analyzed the claim under Article 4A of the Uniform Commercial Code ("UCC"), the law governing wire transfers. Section 4A-202 provides that outgoing wire transfers are effective as the payment orders of a customer, even though the customer did not authorize them, if (i) the bank and the customer agreed that the authenticity of payment orders would be verified pursuant to the security procedure, (ii) the security procedure is "commercially reasonable," and (iii) the bank proves that it accepted the payment orders in good faith and in compliance with the security procedure. The Michigan court found that the security procedure was "commercially reasonable," based on the token technology used by the bank to protect against fraud. However, the court found that even though the security procedure was commercially reasonable, the bank failed to meet its burden of showing that, under UCC § 4A 202, "it accepted the payment order in good faith."

The court concluded that because of the significant irregularities in the account created by the payment orders initiated by the fraudster – such as a $5 million overdraft on an account that normally had a $0 balance – it should have detected and stopped the fraudulent wire activity earlier. The court stated: "The trier of fact is inclined to find that a bank dealing fairly with its customer, under these circumstances, would have detected and/or stopped the fraudulent wire activity earlier. Comerica fails to present evidence from which this court could find otherwise."

In the Maine case, *Patco Construction Company, Inc. v. People's United Bank d/b/a Ocean Bank*,[6] the bank fared much better. In this case, the court did not address the issue of whether the bank had failed to act in good faith as in the Experi-Metal case, because it was never raised by the plaintiff. Indeed, the court focused solely on whether the bank's security procedure was commercially reasonable under UCC 4A-202.

In *Patco*, a number of large unauthorized withdrawals were made from the bank account of Patco Construction Company, a corporate customer of the defendant bank. The bank authenticated the transfers based on the use of the corporate customer's identification, password, customer employee credentials, and answers to three challenge questions. Fraudsters had somehow obtained this information and then initiated transfers from the corporate account to a number of individual accounts. The withdrawals totaled $588,851. The bank was able to block $243,406 of the transfers, but the rest was lost.

The court in *Patco* devoted considerable time examining the security procedure in place at the time of the fraudulent transfers. In concluding that the bank's security procedure was "commercially reasonable," the court noted that the bank had used a vendor's security authentication product that was crafted directly in response to the 2005 Guidance. Because the bank's security procedure was commercially reasonable, it was not required to re-credit its customer's account for the loss.

Conclusion

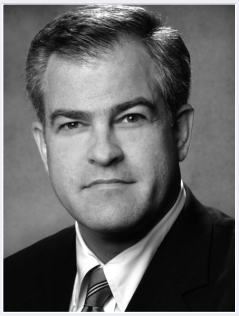
Financial institutions should review their payment authentication procedures in light of the growing cyber fraud threat, the 2011 Guidance, and the increased litigation risks associated with cyber fraud.

* * * * *

1. "Cyber Security: Threats to the Financial Sector," Testimony before the House Financial Services Committee Subcommittee on Financial Institutions and Consumer Credit by Gordon M. Snow, Federal Bureau of Investigation, September 14, 2011.
2. Testimony before the Senate Committee on Banking, Housing, and Urban Affairs by Kevin F. Streff, Associate Professor of Information Assurance, Dakota State University Information Assurance Center, June 21, 2011.
3. Shames-Yeakel v. Citizens Financial Bank, 677 F. Supp. 2d 994 (N.D. Ill. 2009).
4. Patco Construction Company, Inc. v. People's United Bank d/b/a Ocean Bank, No. 2:09-cv-503-DBH, 2011 WL 2174507 (D. Me. May 27, 2011).
5. Experi-Metal, Inc. v. Comerica Bank, No. 09-14890, 2011 WL 2433383 (E.D. Mich. June 13, 2011).
6. Patco Construction Company, Inc. v. People's United Bank d/b/a Ocean Bank, No. 2:09-cv-503-DBH, 2011 WL 2174507 (D. Me. May 27, 2011).

ARIZONA INSURANCE DEPARTMENT PLACES PMI MORTGAGE INSURANCE COMPANY INTO RECEIVERSHIP

On October 20, 2011, the Director of the Arizona Department of Insurance filed a Complaint to place PMI Mortgage Insurance Company (PMI) into receivership in Arizona. In an interim Order, the court required the director, as Receiver, to take possession and control of PMI, which had been under the formal supervision of the insurance department since August 19, 2011. The court also directed that certain related affiliates of PMI be placed under administrative supervision. Reed Smith is forming a group of interested clients to enter an appearance in the Arizona proceedings to ensure that our clients have notice of the proceedings and an opportunity to participate to protect their rights.



Curtis G. Manchester
Partner – Richmond, VA
Commercial Litigation
cmanchester@reedsmith.com

PMI was one of a handful of companies writing mortgage insurance coverage, which insures a lender against loss from a borrower's default on a mortgage loan. PMI currently is paying approved mortgage insurance claims at 50 percent of their value and providing a deferred payment obligation for the remaining 50 percent. This resembles the run-off payment structure used by Triad Guaranty Insurance Corporation, an unrelated mortgage insurance company.

PMI is now under the total control of the Receiver, and there will be a request to place PMI in formal rehabilitation, which distinguishes PMI from Triad. The gap between PMI's assets and liabilities is broad, and is expected to increase. In forming a group of interested mortgage insurance policyholders, our goal is to make sure that mortgage insurance policyholders have a seat at the table when the rehabilitation plan is being formulated and adopted. We expect to address a number of policyholder concerns, including the following:

Captive Reinsurance. Some policyholders have captive reinsurance that reinsures PMI's mortgage insurance obligations to the lenders. The captive reinsurance must be treated appropriately. The proceedings may address whether the captive reinsurance company may elect to directly pay the lender, whether reinsured claims will be treated as "secured claims" in any rehabilitation or liquidation of PMI, and whether PMI can collect from captive reinsurance based solely on its payments or based also on the deferred payment obligation.

Jurisdictional Disputes. The PMI Group, Inc. (PMI Group), PMI's parent, is seeking to regain control of its mortgage insurance subsidiary, and a ruling from the court in Arizona is expected in the near future. On October 24, 2011, PMI Group filed an 8-K Report, noting the effect of the receivership proceedings on its debt obligations. Some observers are concerned that PMI Group will enter bankruptcy proceedings. PMI Group is a Delaware corporation, principally located in California. A bankruptcy filing by PMI Group could lead to jurisdictional issues between the bankruptcy court and the court overseeing the proceedings in Arizona. Policyholders have an interest in ensuring that the assets of the mortgage insurance subsidiary are maximized, and that transactions within the holding company system are scrutinized.

Ensuring Prompt and Fair Claim Payment. Any rehabilitation or liquidation should ensure the prompt and fair payment of claims due under mortgage insurance policies. Unjustified rescissions of coverage are not an acceptable means of increasing solvency.

STATE TAX THOUGHT OF THE DAY: LOOK OUTSIDE THE 'BANK' BOX!

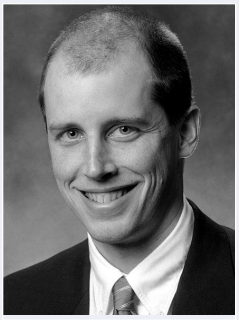
Sara A. Lima
Associate– Philadelphia
State Tax
slima@reedsmith.com

In this era of change for financial institutions, most in the industry have had their hands full with regulatory compliance. Absent big-news legislative amendments, state bank taxes seem to warrant little attention. But some of the state bank taxes in the region rely on regulatory business distinctions between institutions that are fluctuating if not disappearing. (Or taxing authorities are applying them differently because of substantial state budget deficiencies.) These changes can create significant refund opportunities (or exposure) for financial institutions.

One example is the Virginia bank franchise tax. Based on net capital, this tax applies to state and national banks, banking associations, and trust companies. But savings and loan associations ("S&Ls") do not pay bank franchise tax. Instead, S&Ls pay corporate income tax. Several federal and state laws require parity between financial institutions for state tax purposes, including the National Bank Act, the Home Owners' Loan Act, the Equal Protection Clause of the United States Constitution, and the Uniformity Clauses of state constitutions. So, if the corporate income tax (and its bad debt deduction) yields a better tax result for your institution, consider whether your "bank" might be entitled to a refund of the difference between the two.

CONSUMER FINANCE LITIGATION: STRATEGIES FOR HANDLING THE GROWING CATEGORY OF SELF-REPRESENTED PLAINTIFFS

Everyone who regularly works on consumer finance litigation has noticed the dramatic uptick of cases brought by individuals representing themselves, known as pro se plaintiffs. Some of these are attorneys choosing to handle their own cases, but most are lay persons who either cannot afford, do not want to pay for, or cannot find an attorney to represent them. The difficulties in the economy are certainly responsible for a general increase in consumer finance litigation. The economy also likely caused the increase in the percentage of cases wherein plaintiffs are representing themselves, because more people are in financial circumstances that prevent them from retaining counsel for a fee, and the attorneys specializing in representing consumer finance plaintiffs are able to be more selective and must turn people away because there are too many prospective clients. Another obvious cause of the growth in self-representation in consumer finance litigation is the availability of forms (of varying quality) on the Internet that people can use to draft pleadings for their own cases. Some forms are designed to assert frivolous claims such as the "prove I owe you" claims, but others are truly intended to assist the pro se litigant that has a legitimate gripe.



Travis A. Sabalewski
Partner– Richmond, VA
Commercial Litigation
tsabalewski@reedsmith.com

When a new pro se case comes in the door, it is sometimes possible to discern immediately from the initial pleading that it is merely a frivolous case based on a bad form, but more often it is unclear until the account/loan documents are reviewed or after that ever-important first conversation with the plaintiff. Self-represented plaintiffs are sometimes unwilling to talk to opposing counsel out of intimidation and need to be coaxed into it by (true) assertions that we simply want to hear their story and learn what they believe they are entitled to receive as relief in the case. Sometimes the answer is the moon and the stars, and it is possible to discern that this one must be fought in the court. Other times, the plaintiff wants something simple, like a change in how his or her account is being reported to the credit bureaus or a small credit to the account on a legitimate basis. Often this cannot be discerned from the plaintiff's court filing because the filing is not expressed as well in writing. Occasionally, the plaintiff has a truly legitimate and significant basis for a claim, which if it had been handled by experienced consumer finance counsel could have cost the defendant lender a great deal of money, but a proper and legitimate settlement is possible at a much lower level and without the need to incur substantial attorneys fees because the individual is not well represented.

More so than in cases with represented plaintiffs, it is that first phone call in the context of a self-represented plaintiff that sets the tone. It is crucial that the person making that call must have familiarity with the history of the account and cause the plaintiff to trust them. The caller must listen carefully to the plaintiff's description of the dispute, respond in a measured way, and cause the plaintiff to understand that the lender will do what is fair, but nothing more. Whatever questions are raised in the initial call need to be answered quickly and the plaintiff needs to be apprised of the position of the lender. Often the litigation is born of individuals experiencing a "run-around" on telephone systems and call centers. They need to know that someone is now paying attention and will address their legitimate concerns, but will recognize the frivolous issues they raise and reject them. As mentioned above, some cases just have to be fought, but like any other case, there is an opportunity with self-represented plaintiffs to reach a quick and reasonable solution, if care is taken in how that first call is made.

REED SMITH'S GENERAL COUNSEL GROUP — HOW THEY CAN HELP YOU

The Reed Smith General Counsel (RSGC) group is a unique panel of highly experienced former general counsel within Reed Smith who are available to clients for consultation on a variety of issues. RSGC is set up to give you quick and direct access to people who understand the challenges that confront you today, particularly financial services clients. They hail from multi-billion-dollar companies in the financial services industry, and possess an outstanding record of results in bet-the-institution situations. If you are looking for advice on a broad range of issues, including board preparation, crisis counseling, corporate governance, managing outside counsel, or structuring and managing the inside legal function; or if you just want to bounce your thinking off someone—RSGC can be an invaluable resource for you. Combined, Michael Bleier, Carl Krasik and Bill Mutterperl possess more than 35 years of experience as general counsel, leading their respective banks through various business, economic and regulatory environments. We see this as an investment in our client relationship and would offer this service at no cost. To learn more about our RSGC Program, please contact Joseph "Jay" Spruill at jspruill@reedsmith.com.

VIRGINIA-READY Reed Smith is recognized nationally for its representations of financial services clients across a wide array of matters. We are regularly on the leading edge of precedent-setting issues, and we understand the continual shifts in the financial services industry. Our geographic presence in Virginia provides us with the distinct ability to tailor our global experience in an effort to provide unparalleled service at national and regional levels. Our offices in Richmond, Falls Church and Washington, D.C., uniquely position us to serve the needs of Virginia-based financial institutions.

Reed Smith's Financial Industry Group is comprised of more than 220 lawyers organized on a cross-border, cross-discipline basis, and dedicated to representing clients involved in the financial sector, advising most of the top financial institutions in the world. As well as being authorities in their areas of law, FIG lawyers have a particular understanding of the financial services industry sector, enabling the practice to evaluate risks, and to anticipate and identify the legal support needed by clients. Lawyers in the group advise on transactional finance covering the full spectrum of financial products, litigation, commercial restructuring, bankruptcy, investment management, consumer compliance, and bank regulation, including all aspects of regulatory issues, such as examinations, enforcement and expansion proposals.

VIRGINIA AREA OFFICES

Richmond
Riverfront Plaza-West Tower
901 East Byrd Street
Suite 1700
Richmond, VA 23219-4068
Phone: +1 804 344 3400
Fax: +1 804 344 3410

Falls Church
3110 Fairview Park Drive
Suite 1400
Falls Church, VA 22042
Phone: +1 703 641 4200
Fax: +1 703 641 4340

Washington D.C.
1301 K Street, N.W.
Suite 1100, East Tower
Washington, DC 20005-3317
Phone: +1 202 414 9200
Fax: +1 202 414 9299

ReedSmith

The business of relationships.℠

NEW YORK
LONDON
HONG KONG
CHICAGO
WASHINGTON, D.C.
BEIJING
PARIS
LOS ANGELES
SAN FRANCISCO
PHILADELPHIA
SHANGHAI
PITTSBURGH
MUNICH
ABU DHABI
PRINCETON
N. VIRGINIA
WILMINGTON
SILICON VALLEY
DUBAI
CENTURY CITY
RICHMOND
GREECE
OAKLAND

reedsmith.com