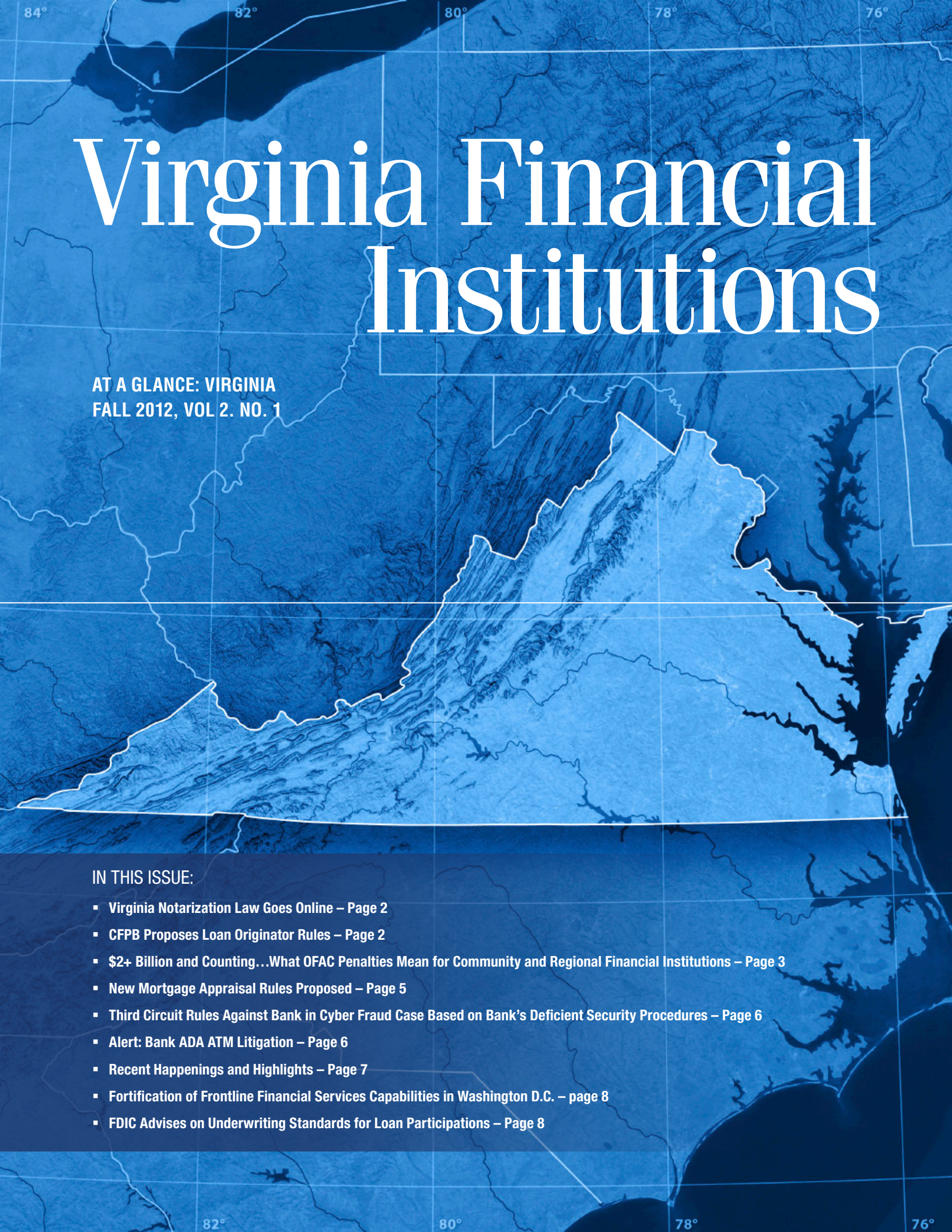

Virginia Financial Institutions

AT A GLANCE: VIRGINIA
FALL 2012, VOL 2. NO. 1

IN THIS ISSUE:

- Virginia Notarization Law Goes Online – Page 2
- CFPB Proposes Loan Originator Rules – Page 2
- $2+ Billion and Counting…What OFAC Penalties Mean for Community and Regional Financial Institutions – Page 3
- New Mortgage Appraisal Rules Proposed – Page 5
- Third Circuit Rules Against Bank in Cyber Fraud Case Based on Bank's Deficient Security Procedures – Page 6
- Alert: Bank ADA ATM Litigation – Page 6
- Recent Happenings and Highlights – Page 7
- Fortification of Frontline Financial Services Capabilities in Washington D.C. – page 8
- FDIC Advises on Underwriting Standards for Loan Participations – Page 8

VIRGINIA NOTARIZATION LAW GOES ONLINE

On July 1, 2012, Virginia became the first state in the country to authorize remote online notarization. Legislative changes to Virginia's notary law[1] that took effect on that date allow a signer in one location to "appear" online before a notary public in another location and have his or her signature on a document notarized electronically. These changes are intended to make the notarization process compatible with today's digital information economy.

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

Many states, including Virginia, already have laws authorizing electronic notarizations. But under these laws the signer must still physically appear before the notary in order to have an electronic document notarized. Virginia's new online notary law is unique in that a signer and a notary can be located in different places. Indeed, a signer anywhere in the world may appear online before a duly commissioned Virginia notary to have his or her signature notarized.

Under traditional notary law, a notary ascertains the identity of the signer by examining such person's state driver's license, United States Passport, or other official identification while in the physical presence of such signer. With electronic notarization under Virginia's new law, "satisfactory evidence of identity" may be based on audio-video conference technology (*i.e.*, webcam) that allows the notary to communicate with and identify the signer at the time of the notarial act, provided such identification is confirmed in one of three ways.[2] Such confirmation may be based on: (1) personal knowledge; (2) reliance on prior in-person identity proofing by a trusted third party (*e.g.*, a bank, title company, law firm); or (3) a valid digital certificate accessed by biometric data or a Personal Identity Verification card issued in accordance with federal government specifications.[3]

In this age of cloud-computing, Virginia's new law will promote efficiencies in the electronic storage of documents. Also, experts say that online notarization is more secure than paper-based notarizations. In this regard, the law requires a notary to keep a copy of the recording of the audio-video conference for at least five years from the date of the transaction; this will deter would-be criminals and provide critical evidence of a criminal's identity when fraud does occur.

Most importantly, the new law provides opportunities for both cost savings (an online notary service is estimated to cost one-half of a paper-based notary process) and new revenue for financial institutions and others that routinely require documents to be notarized.

---

1 Virginia Acts of Assembly, 2011 Session, Chapter 731 and Chapter 834 amending Va. Code § 47.1-2 *et. seq.*

2 Va. Code § 47.1-2.

3 *Id.*

CFPB PROPOSES LOAN ORIGINATOR RULES

By Joseph "Jay" E. Spruill, III, Counsel – Richmond

The Consumer Financial Protection Bureau ("CFPB") proposed rules August 15 to implement provisions in the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act") dealing with mortgage loan originator compensation and qualification requirements for loan originators. The proposed rule is subject to a comment period until October 16, 2012. A final rule is expected early in 2013.

Under the proposed rule, before a lender or mortgage broker could impose upfront points and fees on a consumer in a closed-end mortgage transaction, the lender or broker would have to make available a comparable, alternative loan with no upfront discount points, origination points, or origination fees (the "zero-zero alternative"). This requirement would not be triggered by charges that are passed on to non-affiliated third parties, nor would it apply where the consumer is unlikely to qualify for the zero-zero alternative. In transactions not involving a mortgage broker, if at any time prior to loan application the lender provides a consumer with a quote for a mortgage loan that includes upfront points and/or fees, there is a safe harbor if such lender also provides a quote for a zero-zero alternative.

In transactions that do involve a mortgage broker, there is a safe harbor if lenders provide quotes for all their zero-zero alternatives to the mortgage broker and such broker presents such zero-zero alternatives when presenting different loan options to consumers.

The proposed rule also clarifies that employers may make contributions from general profits derived from mortgage activity to 401(k) plans, employee stock plans, and other "qualified plans" in which loan originators participate, notwithstanding the general Dodd-Frank Act ban on loan originator compensation that is based on mortgage loan transaction terms. In addition, the proposed rule would permit employers to pay bonuses or make contributions to non-qualified profit-sharing or retirement plans from general profits derived from mortgage activity if either: (1) the loan originator affected has originated five or fewer mortgage transactions during the past 12 months; or (2) the company's mortgage business revenue is limited to a certain percentage. In this regard, the CFPB is proposing two alternatives for this revenue limitation: 25 percent or 50 percent of total revenues.

The proposed rule would require that all loan originators and their employers be "qualified" and put their license or registration numbers on certain specified loan documents. In particular, where a loan originator is not already required to be licensed under the SAFE Act (e.g., depository institution employees), the proposed rule would require the employer to ensure the loan originator meets character, fitness, and criminal background check standards that are the same as would apply under the SAFE Act, and that such loan originator is appropriately trained. In this regard, employers would be required to ensure that their loan originator employees are licensed or registered under the SAFE Act where applicable.

Finally, the proposal prohibits mandatory arbitration provisions in mortgage loan agreements and the financing of premiums for credit insurance.

$2+ BILLION AND COUNTING… WHAT OFAC PENALTIES MEAN FOR COMMUNITY AND REGIONAL FINANCIAL INSTITUTIONS

Continuing a trend that has been developing for a few years, headlines were again captured this summer by allegations of U.S. sanctions violations and related money laundering against well-known financial institutions. Most notably, on June 12, 2012, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") announced that it had reached a $619 million settlement with ING Bank N.V. ("ING") relating to potential liability under various U.S. sanctions against Burma (Myanmar), Cuba, Iran, Libya, and Sudan.[1] The settlement was the largest in a string of enforcement actions relating to financial institutions' compliance with U.S. sanctions.

Just this summer, in addition to the ING settlement, we have seen the release of a Congressional report detailing allegations of money laundering and OFAC sanctions violations by a prominent financial institution, and the aggressive enforcement of sanctions-related allegations by New York's Department of Financial Services against one of the world's largest financial institutions. OFAC cases will continue to capture the attention of U.S. and foreign regulators and will have a significant impact on the stakeholders of financial institutions for many years to come. With more than $2 billion in penalties during the past few years and no sign of slowing down, this issue is too big to ignore.

Michael J. Lowell
Associate – Washington, D.C.
Global Regulatory Enforcement
mlowell@reedsmith.com

Background

OFAC administers and enforces economic sanctions against targeted foreign countries, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other perceived threats to the national security, foreign policy, or economy of the United States. The sanctions prohibit or restrict U.S. persons from engaging in transactions involving certain countries, groups, and individuals.

OFAC currently administers comprehensive economic sanctions against Cuba, Iran, Sudan, and Syria. OFAC also administers more limited sanctions targeted at current or former governments, persons or entities linked to the Western Balkans, Belarus, Burma (Myanmar), Cote d'Ivoire (Ivory Coast), Democratic Republic of the Congo, Libya, North Korea, Somalia, and Zimbabwe, as well as limited sanctions related to Iraq and Lebanon. In addition, OFAC administers targeted sanctions against certain specified narcotics traffickers, terrorists, and weapons proliferators, and prohibits U.S. persons from engaging in transactions with any individual or entity listed on OFAC's List of Specially Designated Nationals and Blocked Persons (the "SDN List").[2]

The sanctions limit the ability of U.S. persons to engage in transactions. A "U.S. person" is a "United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States." *See, e.g.*, 31 CFR § 538.315. Each sanction regime is different, however, and the prohibitions contained therein are distinct. For example, the Cuban sanctions prohibit transactions of U.S. persons, as well as their foreign subsidiaries. In comparison, until very recently, the Iranian sanctions did not prohibit transactions by foreign subsidiaries[3] of U.S. companies, and the Sudan and Syria sanctions programs generally still do not apply to foreign subsidiaries of U.S. companies.[4]

The fines for violations of OFAC sanctions can be substantial. Depending on the program, criminal penalties can include fines ranging from $50,000 to $10 million per violation, and imprisonment ranging from 10 to 30 years for willful violations. Depending on the program, civil penalties range from $250,000 or twice the amount of each underlying transaction, to $1,075,000 for each violation.

OFAC Enforcement against Banks and Financial Institutions

OFAC's enforcement priority has been squarely focused on financial institutions for a number of years. The recent cases often relate to the removal of material information from wire transfers (so-called "stripping"), insufficient diligence with regard to letters of credit, transactions involving blocked property, and investments in funds owned or operated by SDNs. These OFAC violations are often paired with allegations of money laundering or violations of other financial regulatory requirements, such as the Bank Secrecy Act.

While most of the recent published cases have been directed at European-based, global financial institutions, recent penalties have also been assessed against a small community bank[5] and a domestic investment management firm.[6] Historically, there have been a number of OFAC enforcement actions involving community and regional financial institutions. The published cases indicate a series of OFAC enforcements in the early 2000s against domestic regional and community banks and financial institutions for allegations largely relating to funds transfers and operation of accounts for sanctioned persons. Also, there have been numerous unpublished voluntary disclosures, subpoenas, and investigations that have affected community and regional financial institutions.

There have also been recent enforcement actions in activities that are commonly considered to be low-risk for sanctions violations, such as purely domestic or local activity. For instance, a Dallas homeowners association was penalized earlier this year for reimbursing itself for past assessments and late fees from the sale of property in which an SDN had an interest.[7] More recently, OFAC has settled an enforcement action with Great Western Malting Co. where liability was based solely on the back-office support that Great Western's U.S.-based employees provided for a foreign affiliate's sales to Cuba.[8]

What Do These Cases Mean for You?

Community and regional banks will be expected to understand the types of issues that led to the violations in these cases, and to ensure that their existing compliance programs are designed to minimize associated risks. In many of the enforcement actions, OFAC found management indifference or involvement, weak internal controls, widely used "work-arounds" to avoid delays (circumvent U.S.

(continued)

$2+ Billion and Counting…What OFAC Penalties Mean for Community and Regional Financial Institutions—continued from page 3

bank filters), and the failure of bank employees to respond to "red flags." In many cases, the financial institutions had compliance programs, but the programs were "stale," not fully implemented, or otherwise ineffective.

Community and regional banks and financial institutions should be periodically considering a few key questions:

- ***OFAC Risk Assessment*** – Do we understand where our risks exist? Have we considered how those risks have changed over time? Have we reviewed current risks or are our assessments based on risks at the time we implemented our compliance program?
- ***Industry Benchmarking*** – The "stripping" cases certainly stand for the proposition that widespread industry practice is no excuse, but it is still important to understand where we fit in relation to peer institutions. Do we know what our competitors are doing to ensure compliance? Do we know what the market leaders are doing? Have we adopted an approach that is consistent with industry leaders? Are there ways we can improve efficiency without decreasing controls?
- ***Blocked/Rejected Transactions*** – As OFAC has said, "If your bank does not block and report a transfer and another bank does, then your bank is in trouble." Do we have a system in place for ensuring that blocked transactions are timely reported? Do we audit our systems to ensure that they are working properly? Do we have a clear reporting chain within our organization to ensure that appropriate personnel are notified? Do we have gaps in our program? Is an override possible? If so, who has the ability to override and are they properly trained?
- ***Software Filtering*** – Most banks have software solutions that provide filtering for SDNs and other persons who may be prohibited or blocked under U.S. law. Do we have a solution? Do we have gaps in our solution like the gap noted in the Trans Pacific settlement? Are there any gaps in implementation? Do we have a rationale basis for setting filters at different sensitivity settings? Who is reviewing screening hits? Are they adequately trained? Do they have a defined process for resolving screening hits? Can we make this process more efficient?
- ***Compliance Program*** – Are responsibilities clearly delineated in our compliance program? Are personnel adequately trained? Are employees bogged down with the existing program – can we make it work better? Does our program have manual and electronic elements? Have we evaluated the sufficiency of our program in the past five years? Ten years? Are we relying on a program that was implemented when we first learned of these issues? Have changes in the financial reporting requirements and sanctions been implemented?
- ***Policies and Procedures*** – Do we have written policies and procedures? Are they current? Is anyone using them? Where are they stored, how are they communicated, and who needs them? Do we have processes for ensuring compliance with vendors and partners? Have we audited compliance with the procedures and policies? Do we have a clear policy (and a clear management commitment) to compliance with the sanctions?
- ***Training*** – Are responsible personnel attending training? Have business leaders and management been briefed on requirements? How widespread should training be? How often should training occur? How is information about changes in the law shared with personnel?
- ***Auditing*** – Are we auditing for OFAC compliance and effectiveness of our OFAC compliance program? Do we need internal or external auditing? Have our internal auditing departments uncovered past noncompliance? What have we done to address this and have we considered a voluntary disclosure?

These questions and many more should be periodically answered to ensure that all financial institutions have an appropriately tailored, risk-based approach to compliance with the sanctions.

Conclusion

OFAC's continued enforcement focus on financial institutions and its demonstrated willingness to second-guess risk-based compliance approaches (such as in OFAC's enforcement against GEICO[9]) requires financial institutions of all sizes and scope to continue to monitor developments in the law, and changes in industry practices, and to approach OFAC issues with great care. As the requirements under the sanctions administered by OFAC have changed over time and have become more intertwined with other financial services regulations, the risks associated with an OFAC violation have increased considerably. Indeed, companies alleged to have violated the sanctions are now often left facing enforcement prosecutions and investigations by various federal agencies (OFAC, SEC, DOJ), state and local officials, and foreign governments. The questions above should help you focus your attention on where your compliance program may have shortcomings or gaps.

———————————

1 http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20120612.aspx.

2 More information about OFAC's various sanctions programs can be found here: http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx.

3 *See*, *e.g.*, 31 C.F.R. § 515.329(d).

4 31 C.F.R. § 560.314; Iran Threat Reduction and Syria Human Rights Act of 2012, H.R. 1905.

5 Trans Pacific National Bank allegedly violated U.S. sanctions on Iran by initiating two wire transfers on behalf of an account holder who was engaged in commercial transactions relating to Iran. OFAC noted the failure of the bank's internal filtering system since the system was not designed to detect references to sanctions targets in memorandum information fields of wire transfers. Trans Pacific remitted $12,500 and enhanced its compliance program.

6 Genesis Asset Managers, LLP, a U.S. investment manager for a foreign investment fund, delegated investment authority to its foreign subsidiary in London. The foreign subsidiary invested in foreign-owned assets in a Cayman Islands investment fund that in turn invested in Iranian securities. Genesis was apparently not involved in any of the investment decisions. Apparently, OFAC's enforcement theory was that Genesis delegated its investment authority to its foreign subsidiary without having sufficient controls in place to ensure compliance with OFAC's sanctions. Genesis agreed to remit $112,500 to settle its potential liability.

7 http://www.treasury.gov/resource-center/sanctions/CivPen/Documents/02172012_richland.pdf.

8 http://www.treasury.gov/resource-center/sanctions/CivPen/Documents/07102012_great_western.pdf. For more information, see: http://www.globalregulatoryenforcementlawblog.com/2012/07/articles/export-customs-trade/us-companys-backoffice-support-of-a-foreign-affiliates-sales-in-cuba-leads-to-ofac-sanctions-penalty/.

9 http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Documents/06032010.pdf.

NEW MORTGAGE APPRAISAL RULES PROPOSED

Two proposals to implement new appraisal standards under the Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Dodd-Frank Act") were released by federal financial agencies on August 15. The first would establish new appraisal requirements for higher-risk mortgage loans. The second would increase consumer access to appraisal and valuation reports in all first-lien mortgage transactions. Both proposals are subject to a 60-day comment period, and are expected to be finalized by early next year.

Appraisals for Higher-Risk Mortgage Loans

Under this proposal, which was issued jointly by six federal financial regulatory agencies and would amend Regulation Z (Truth-in-Lending), a creditor may make a "higher-risk mortgage loan" only if it follows certain new conditions regarding the appraisal of the real property securing the loan. A "higher-risk mortgage loan" is generally defined as a closed-end consumer credit transaction secured by a principal dwelling with an annual percentage rate that exceeds the "average prime offer rate" ("APOR") by 1.5 percent for a first-lien loan, 2.5 percent for a first-lien jumbo loan, and 3.5 percent for a subordinate-lien loan. (The APOR is determined by the Consumer Financial Protection Bureau based on average interest rates, points, and other loan pricing terms for low risk loans by a representative sample of mortgage lenders.) The proposed rule would exclude from the definition of "higher-risk mortgage loan" the following: a "qualified mortgage," yet to be defined under the "ability-to-repay" regulations; a reverse mortgage; and a loan secured solely by a residential structure.

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

The proposed rule would require a lender making a higher-risk mortgage loan to obtain an appraisal from a certified or licensed appraiser. That appraiser would be required to make a physical inspection of the interior of the residence in connection with such appraisal.

The proposed rule provides that the creditor would have to provide the consumer with a statement at loan application regarding the purpose of the appraisal, that the creditor will provide the applicant with a copy of any written appraisal report, and that the consumer may choose to have a separate appraisal done at the consumer's expense. The lender would be required to provide a free copy of the appraiser's report at least three business days before closing.

The proposed rule would require a lender to obtain a second appraisal from an equally qualified appraiser, at no cost to the consumer, under certain circumstances. This requirement is intended to prevent fraudulent property flipping. In particular, a second appraisal would be required where: (i) the higher-risk mortgage loan would finance the purchase of the consumer's principal residence; (ii) the seller of the residential property acquired such property less than 180 days before the date of the consumer's purchase contract; and (iii) the consumer is paying more than the seller paid.

The second appraisal would have to be performed by another appraiser and would have to analyze the difference in prices, any changes in market conditions, and any improvements made by the seller.

Mandatory Disclosure of Written Appraisals and Valuations

The Consumer Financial Protection Bureau ("CFPB") has proposed regulatory changes to implement amendments made to the Equal Credit Opportunity Act ("ECOA") under the Dodd-Frank Act. In particular, the CFPB's proposal would amend Regulation B, which implements ECOA, to require creditors to provide first-lien mortgage applicants with a copy of all written appraisals and valuations promptly after receiving an appraisal or valuation, but in no case later than three business days prior to the closing of the mortgage. Regulation B currently allows a creditor to provide an appraisal report only if requested by the applicant.

In addition, the proposal would require creditors to notify an applicant, within three business days of receiving his or her application, of that person's right to receive a copy of the written appraisal or valuation developed in connection with the application. The proposal would allow an applicant to waive the requirement to receive the appraisal within three business days prior to consummation of the mortgage, but the applicant who waives this requirement would still be entitled to a copy of the written appraisal or valuation at or prior to closing. Finally, the proposed new rules would prohibit creditors from charging additional fees for providing a copy of a written appraisal or valuation, but a creditor could still seek reimbursement for the cost of the appraisal or valuation unless otherwise required by law.

Importantly, the proposal broadens the scope of the current requirement to provide copies of "an appraisal report" to include "all written appraisals and valuations developed." "Valuation" is defined under the proposed rules as "any estimate of the value of a dwelling developed in connection with a creditor's decision to provide credit." Hence, the proposed rule covers more types of documents that would have to be provided to the loan applicant. It should also be noted that the proposed rule would apply to applications for credit to be secured by a first lien on a dwelling. The current rule applies to credit secured by a first lien or subordinate lien on a dwelling.

THIRD CIRCUIT RULES AGAINST BANK IN CYBER FRAUD CASE BASED ON BANK'S DEFICIENT SECURITY PROCEDURES

On July 3, 2012, the United States Court of Appeals for the Third Circuit ruled that a commercial customer could proceed against its bank for $345,000 in losses that the customer suffered in a cyber fraud attack. The Third Circuit based its decision on the bank's failure to maintain "commercially reasonable" security procedures. The case, *Patco Construction Co., Inc. v. People's United Bank*,[1] reversed a lower court's grant of summary judgment in favor of the bank.[2] This is the first time a federal appeals court has addressed the sensitive issue of bank liability for account losses resulting from cyber fraud.

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

Under the facts of the case, Patco, a family-owned construction company, maintained a commercial deposit account at the bank from which it routinely initiated electronic funds transfers through the account's Internet banking ("eBanking") function. Patco primarily used the account to make payroll payments. The highest payment Patco ever made using eBanking was approximately $36,000. Such payments were always made on Fridays, and were initiated from one of the business computers at Patco's offices. The origination of such transfers was always from a single static Internet Protocol ("IP") address.

The bank used a vendor, Jack Henry & Associates, to help implement security procedures in accordance with the Guidance from the Federal Financial Institutions Examination Council ("FFIEC") entitled "Authentication in an Internet Banking Environment."[3] Based on the FFIEC's Guidance, the bank determined that its eBanking product was a "high risk" system that called for greater security, and, in particular, multifactor authentication. Under Jack Henry's multifactor authentication program provided to the bank, when a customer logged in, it was required to enter an ID and password for the company and an ID and password for the individual user. The program also included, among other things, challenge questions that were triggered when a transaction was more than a certain amount, and "risk scoring," which relied on a number of different factors, including the location from which a user logged in, and the size, type, and frequency of payment orders normally issued by the customer. Importantly, about a year before the transactions at issue in the case, the bank lowered the dollar amount threshold for challenge questions from $100,000 to $1.

A series of unauthorized withdrawals was made from Patco's account over several days in May 2009. Cyber criminals had apparently hacked into Patco's computer system to obtain login and password information, along with answers to challenge questions, and then used this information to withdraw more than $588,000 from the account. Of this amount, the bank was able to block $243,000 of the transfers.

The withdrawals were directed to go to accounts of numerous individuals, none of whom had previously been sent money by Patco. The perpetrators logged in from a device unrecognized by the bank and from an IP address that Patco had never used. The risk-scoring engine the bank maintained generated a substantially higher risk-score in connection with the transactions because they were inconsistent with the timing, value, and geographic location of Patco's regular payment orders. Nevertheless, the bank failed to monitor these transactions or notify Patco.

In addressing the question of the bank's liability, the court looked to Article 4A of the Uniform Commercial Code ("UCC"), which governs the rights, duties, and liabilities of banks and their commercial customers with respect to electronic funds transfers. Section 4A-1203 of UCC Article 4A provides that if a bank and its customer agree that the authenticity of payment orders issued by the customer

(continued)

ALERT: BANK ADA ATM LITIGATION

Since mid-April 2012, more than 50 putative class action lawsuits have been filed against more than 50 different banks in federal court by Carlson Lynch, a Pittsburgh law firm. In each case, a blind individual plaintiff has sued under the Americans with Disabilities Act of 1990 (ADA) claiming primarily that the bank's automated teller machines (ATMs) are not compliant with the ADA and its implementing regulations because of the lack of voice guidance technology or because the voice guidance malfunctioned.

This wave of class action litigation against the banking industry follows the U.S. Department of Justice's issuance of new Standards for Accessible Design on September 15, 2010. ATMs had to be upgraded to include voice guidance by March 15, 2012.

While financial institutions already have expended significant amounts of capital to purchase new ATMs or upgrade existing ones, and deploy voice guidance technology promptly and efficiently, the industry has faced ATM supply shortages and an inadequate supply of technicians to complete the installations. This has created a window of opportunity for plaintiffs' counsel to create a cottage industry of lawsuits.

Initially, a number of banks settled by entering into formal consent decrees. However, as explained by Roy Arnold, a partner at Reed Smith LLP who has been retained to defend 10 of these cases so far, the banks have successfully resisted consent decrees more recently: "Our clients have resolved a number of these cases without entering into a consent decree. A consent decree is enforceable by a motion for contempt and could lead to monetary penalties for non-compliance. It is a much better outcome for the bank to be able to avoid a consent decree and resolve the case cost-effectively."

Third Circuit Rules Against Bank in Cyber Fraud Case Based on Bank's Deficient Security Procedures—continued from page 5

will be verified pursuant to a security procedure, then a payment made in accordance with such security procedure shall be effective provided the security procedure is "commercially reasonable" and the bank accepts any such payment order in good faith.

The eBanking Agreement between the bank and Patco generally provided that the use of the password with the account constituted authentication for all transactions initiated on the account, and that the bank did not "assume[ ] any responsibilities" with respect to Patco's use of eBanking.

Despite the protection afforded the bank under the eBanking Agreement, the Third Circuit ruled against the bank based on its failure to employ commercially reasonable security procedures. The court held that the bank's lowering of the challenge-questions threshold to $1 substantially increased the risk of fraud, particularly for a customer like Patco that initiated frequent transfers, since it meant that the bank's customer would be entering answers to the challenge questions on virtually every transaction, thereby giving fraudsters using key logging devices more opportunities to steal log-in information. In this regard, the court focused on the commentary to section 4A-1202(3) that requires banks to consider "the circumstances of the customer" known to the bank, such as "the size, type and frequency of payment orders normally issued by the customer to the bank." In Patco's case, according to the court, "these characteristics were regular and predictable," in that Patco used its account primarily for payroll. The bank apparently never offered customers, like Patco, the option to adjust the threshold amount for challenge questions. The court found that the use of a "one-size-fits-all" approach to customers with respect to the challenge questions violated Article 4A's mandate to take into account the unique circumstances of a particular customer.

In addition, the bank failed to respond to the high risk-score when the fraudulent transactions were occurring by closely monitoring those transactions and notifying Patco before allowing them to take place. These transactions were completely uncharacteristic of Patco's normal transactions in that they originated from computers and IP addresses that Patco had never used and were for amounts significantly higher than Patco's normal funds transfers. And yet the bank failed to take advantage of its security program, which identified these discrepancies, by immediately alerting Patco.

The court noted that Jack Henry's risk-scoring system was designed to trigger an additional layer of authentication, such as challenge questions, in the event of a high score indicating unusual or suspicious transactions. Because the challenge questions in this instance were already used, the risk-scoring system was deprived of its core functionality.

In addition, the court noted that the bank's security measures fell below industry standards, such as manual review, tokens, or some other additional security measure.

The case has important lessons for banks seeking to have commercially reasonable security procedures in connection with their Internet banking services:

- Banks may not be able to simply rely on customer agreements that shift the risk of loss to the customer, to avoid liability for cyber attacks
- Banks should consider additional security measures and procedures, including an effective plan to communicate with customers, such as by red-flag emails, when there is suspicious activity
- Banks need to develop and adjust security procedures based on current risks and industry standards
- Banks need to take the individual circumstances of a particular customer into account in its security measures
- Once banks have put in place security measures, they need to take care to follow them

———————————

1 *Patco Const. Co., Inc. v. People's United Bank*, 648 f.3D 197 (1st Cir. 2012)

2 *Patco Const. Co., Inc. v. People's United Bank*, 2010 WL 2174507 (D.C. Me. 2011)

3 The FFIEC updated this Guidance in 2011. *See* our analysis of the new Guidance in the Fall 2011 edition of this report.

RECENT HAPPENINGS AND HIGHLIGHTS

Our VA/DC team of Financial Services lawyers provide counsel and advice on a comprehensive array of matters that are crucial to financial institutions and their success. Some of the recent happenings and highlights from our VA/DC offices include:

- Retained to represent a major bank in an SEC investigation into the sale of $1.6 billion of asset-backed securities
- Representing a mutual fund client in an ongoing fund reorganization, as well as an ETF client in the registration and launch of several new exchange-traded funds on the NYSE Arca
- Advising on the refinance of a $1.86 million loan in a real estate matter
- Advising on a real estate acquisition and related financing deal with a $4.1 million loan from a major lender
- Sandy Thomas named Head of Firmwide Litigation department
- Hosted client dinner in conjunction with the MBA regulatory conference in Washington D.C.
- Hosted guest speaker Dr. Angel Cabrera, new president of George Mason University, for 5th installment of the Beltway Leadership Roundtable series in Falls Church
- Hosted a joint event with 85 Broads and guest speaker Kathleen Casey, former SEC Commissioner in Washington D.C.
- Spoke at a conference sponsored by the UK Ministry of Defense and local UK industry on the topic of Export Compliance Under the New UK/U.S. Cooperation treaty
- Conducted export compliance due diligence for a portfolio company of a private equity firm

FORTIFICATION OF FRONTLINE FINANCIAL SERVICES CAPABILITIES IN WASHINGTON D.C.

Leonard A. Bernstein
Partner–Princeton/Philadelphia
Global Chair, Financial
Services Regulatory Group
lbernstein@reedsmith.com

Adding to our Washington D.C.-based financial services team, Victoria Holstein-Childress recently joined our Financial Services Regulatory Group bringing with her a strong track record of representing financial services institutions and other corporate and individual clients in complex, high-stakes civil litigation and government enforcement actions. Victoria's core emphases include mortgage-related and credit card class actions, and related government and regulatory investigations and enforcement proceedings. Victoria expands the depth of our D.C. Financial Services Team, giving Reed Smith even stronger "inside the beltway" capabilities. Combined with the recent addition in D.C. of other top FIG attorneys to our already strong firmwide financial services practice, her arrival provides further strength in an area where our financial services clients' needs are continuing to grow.

In addition to Ms. Holstein-Childress, Reed Smith's growing D.C. Financial Services Team includes Mary T. Payne, W. Thomas Conner, Terence M. Healy, Timothy J. Nagel, Leigh T. Hansson, Rana J. Wright and Tyree P. Jones.

Ms. Payne joined the D.C. FIG practice in April from Sutherland Asbill & Brennan, where her practice focused on representing financial services clients in a broad range of legal and regulatory issues relating to securities laws. She re-joined her former Sutherland colleague, W. Thomas Conner, with whom she has continued to build a robust practice specializing in commodities-based and securities-based exchange traded funds (ETFs), and variable annuity and life insurance investment products. Mr. Conner joined Reed Smith's FIG as a partner in the Washington, D.C., office in January.

Mr. Healy, a former assistant chief litigation counsel at the U.S. Securities and Exchange Commission, joined Reed Smith's Washington, D.C., office in May; Mr. Nagel, a leading data security expert and former assistant general counsel and chief security officer at Bank of America, joined the office in July.

Ms. Hansson is the leader of Reed Smith's Export, Customs & Trade Team and focuses her practice on international trade and government contracts; Ms. Wright practices in the area of Investment Management focusing on all aspects of investment company and investment advisor regulation and compliance; and Mr. Jones is a trial lawyer focusing on complex class action litigation, including fair lending matters.

Top row (left to right): Mary T. Payne, Terence M. Healy, Victoria Holstein-Childress, Tyree P. Jones; *seated:* W. Thomas Conner, Timothy J. Nagle; *not shown:* Leigh T. Hannson, Rana J. Wright

"In the area of financial services representation, this office now has all the bases well covered with a deep bench of this indus-try's top attorneys," said A. Scott Bolden, Reed Smith's Washington, D.C., Managing Partner.

FDIC ADVISES ON UNDERWRITING STANDARDS FOR LOAN PARTICIPATIONS

By Joseph "Jay" E. Spruill, III, Counsel – Richmond

In a September 12 advisory, the FDIC has told state nonmember banks purchasing loan participations that they should underwrite and administer such participations in the same diligent manner as if they were being directly originated by the purchasing bank. The FDIC's advisory indicates that the over-reliance on lead institutions has in some cases led to significant credit losses for purchasing banks and has contributed to bank failures, particularly where the participation relates to loans to out-of-territory borrowers, and borrowers that are involved in industries unfamiliar to the purchasing bank.

The advisory indicates that, in connection with loan participations, banks should implement an appropriate credit risk management framework that includes:

- Loan policy guidelines that cover origination and purchase decisions, borrower due diligence, an assessment of the purchasing bank's contractual rights and obligations, and a consideration of commitment limits for aggregate purchased participations, out-of-territory participations, and loans originated by lead institutions
- Written loan participation agreements describing the duties of the lead institution, requiring timely borrower credit information, addressing remedies upon default, and outlinining dispute resolution procedures
- Independent credit and review analysis that is the same as if the bank were the originator
- An enhanced due diligence process for out-of-territory or unfamiliar market loan participations

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 210 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

reedsmith.com