P&G Banking

A D V I S O R

Fall 2013

Taking stock of inventory

Are any of your borrowers using slick fraud tricks?

Get ready for new mortgage rules

BANK *Wire*

Social media risks shouldn't be ignored

P&G Associates

www.pandgassociates.com 877.651.1700

Social media risks shouldn't be ignored

In recent years, business use of social media has exploded. Many companies, including banks, are using Facebook, Twitter, LinkedIn and other social media platforms to interact with customers and prospects and to market their products and services. For banks, the opportunities these platforms provide also come with significant risks.

Whether or not your bank has embraced social media, you can bet that many of your employees and customers are using it. So it's critical to develop a plan for managing these risks.

What are the risks?

Earlier this year, the Federal Financial Institutions Examination Council (FFIEC) issued proposed guidance on managing social media risk. The guidance outlines several areas of potential risk, including:

Compliance and legal risks. If your bank uses social media to market or originate deposit or lending products, it's critical to ensure that social media activities comply with applicable laws and regulations.

For example, the Truth in Savings Act requires certain disclosures in connection with ads that use terms such as "bonus" or "APY" (annual percentage yield). A social media posting that includes such terms without making these disclosures (for example, by including a link to the required information) may violate the law. The Truth in Lending Act imposes similar disclosure requirements.

> Even if your bank isn't actively using social media, it can have a negative impact on your bank's reputation.

Social media also may pose a risk of violating fair lending laws. For example, the Equal Credit Opportunity Act and regulations generally prohibit lenders from requesting information about a borrower's race, color, religion, national origin or sex. But social media sites often collect this information. Banks that use these sites should take steps to ensure that they don't improperly request, collect or use this information or give the appearance of doing so.

Careless social media posts also may violate laws that prohibit unfair or deceptive advertising.

Reputation risk. Even if your bank isn't actively using social media as a business tool, social media activity can have a negative impact on your bank's reputation. Dissatisfied customers or other consumers may post negative comments about your bank or accuse it of deceptive marketing or other unlawful practices. Employees may make inappropriate statements. Disgruntled employees and other fraudsters posing as bank officials may portray the bank in a negative light.

It's critical for banks to have policies and procedures in place to monitor these activities and address any negative publicity.

Operational risk. Like other information technology systems and processes, social media presents certain operational risks, including those associated with malware, viruses, data breaches and other dangers that may threaten the security of sensitive customer or bank information.

A related issue is employee use of online file-sharing applications, which can create significant data security vulnerabilities if not controlled. (See "Watch out for file-sharing apps" below.)

What should you do?

The FFIEC recommends that banks develop risk management programs designed to identify, measure, monitor and control social media risks.

These programs should include the following components:

- A governance structure with clear roles and responsibilities for the board and senior management to direct social media strategy and use,
- Policies and procedures for the use and monitoring of social media and compliance with consumer protection laws,
- A due diligence process for selecting and managing third-party providers of social media services,

- Employee training on the bank's policies and procedures regarding work-related use of social media, and
- An oversight process for monitoring information posted to social media sites.

In addition, banks should establish audit and compliance functions to ensure ongoing compliance and prepare periodic reports to the board and senior management on the social media program's effectiveness.

Assess your risk

The complexity of a bank's risk management program depends on its level of involvement in social media. To define the scope of your bank's program, a risk assessment is a good place to start. ▲

Watch out for file-sharing apps

Online file-sharing apps, such as Dropbox, have become wildly popular. They make it easy for people to store important documents in the cloud and share them among multiple devices and even with other people. While these apps are convenient, their use by bank employees can create data security risks.

Regulators expect banks to exercise a high degree of due diligence and implement strict controls when dealing with third-party cloud computing providers. But file-sharing apps often bypass these protections and a bank's IT personnel may not even know about them.

It's critical for a bank's IT policies to address the use of file-sharing apps. Often, the best solution is to provide employees with a secure, enterprisewide file-sharing system.

Taking stock of inventory

Are any of your borrowers using slick fraud tricks?

The New York Attorney General's office in July announced that employees of a Brooklyn medical supply company had been indicted on charges of grand larceny. The scam involved allegedly billing Medicaid more than $1.7 million and a health insurer for Medicaid recipients another $1.5 million for dispensing nearly a million units of a highly specialized, expensive liquid pediatric nutritional formula for children.

In fact, the company didn't dispense any of the expensive formula. According to the Attorney General's office, if it dispensed anything at all, it was a far less costly, common over-the-counter formula. Investigators discovered the fraud after finding none of the expensive formula in the company's inventory.

Fraud involving inventory, in one way or another, happens regularly. Knowing what tricks are employed, and how to trip them up, is half the battle.

Inventory is an easy target

Fraudsters target inventory for several reasons. It's often a borrower's most valuable and largest asset. Moreover, accounting for inventory requires a significant number of complex journal entries, especially for manufacturers and construction firms — a perfect opportunity for burying fictitious journal entries. And inventory is the most difficult area to audit unless the independent accountants are familiar with the industry.

Worse, company insiders have an intimate knowledge of what goes into inventory, including direct labor costs, percentage of completion estimates and overhead allocations. They might try to pull the wool over an unsuspecting auditor's eyes.

Cooking the books is common

Some frauds entail theft or the personal use of inventory items or scrap materials. But larger, more complex inventory ploys happen when a dishonest owner or employee hides embezzlement by booking fictitious journal entries to the inventory account.

When manipulating inventory records, fraudsters typically overstate ending inventory and understate cost of sales. Consider this equation:

Cost of sales = beginning inventory + purchases – ending inventory

The higher the ending inventory quantity is, the lower the cost of sales will be. This is a win-win for borrowers, because collateral values and profits are both boosted by inventory fraud.

Pumped-up numbers are telltale

Fraudsters have been using inventory to hide illegal behavior for decades. In the 1960s, the Allied Crude Vegetable Oil Refining Company overstated salad oil inventory by filling vats with water and adding a thin layer of oil to the tops of vats using underground pipes. The owner pledged $175 million of phantom salad oil as loan collateral before getting caught.

In the late 1980s, struggling disk drive manufacturer MiniScribe created phantom inventory by filling boxes with bricks. The auditors counted the boxes when testing inventory without bothering to open the cartons to confirm the contents.

Phar-Mor grossly inflated computer-generated inventory registers at some locations. Many of the stores had nearly empty shelves.

A more modern twist was used by Phar-Mor in the 1990s. Here, the auditors told management which stores they would visit at year end, and these stores then produced meticulous inventory records. But the company grossly inflated computer-generated inventory registers at the remaining locations. Many of the untested stores had nearly empty shelves, despite their robust computer records.

Fraudsters might also fluff up inventory by inflating unit costs or mismatching units of measure when booking direct materials.

They have also been known to alter employee timesheets or create phantom employees to overstate direct labor costs.

Other cons include manipulating overhead allocations to prematurely release overhead into cost of sales, overvaluing obsolete inventory, double counting items, and including "bill and hold" sales and consignment inventory in physical counts.

Some fraud scams require collusion with an outsider. A supplier, for example, might agree to inflate prices on an invoice or a customer might falsify confirmations for a kickback.

Investigate and verify collateral pledges

When a borrower pledges inventory as loan collateral, you have some work to do. Naïveté about inventory scams can lead to lenders getting burnt, so keep your eyes open to possibilities of fraud. Verify, as much as you reasonably can, the legitimacy of collateral pledges. ▲

Get ready for new mortgage rules

Community banks should begin preparing now for new mortgage rules that take effect on Jan. 1, 2014. The rules, finalized by the Consumer Financial Protection Bureau (CFPB) last January, are designed to protect consumers from risky lending practices.

The CFPB in July made several amendments to the rules, including easing certain requirements for smaller banks. Here are the highlights.

Ability-to-repay rule

The ability-to-repay (ATR) rule, which amends Regulation Z, requires most lenders to make a reasonable, good-faith determination of a borrower's ability to repay a mortgage. The rule prohibits "no-doc" and "low-doc" loans, instead instructing lenders to document and consider certain underwriting standards, including current income or assets, employment status, credit history, monthly expenses, and debt-to-income ratio (DTI).

Lenders must evaluate a borrower's ability to repay principal and interest over the long term. So, for example, if you employ teaser rates the ability to repay must be calculated using the undiscounted interest rate and payment amount.

Qualified mortgage rule

Evaluating each borrower's ability to repay can be burdensome, but the CFPB provided a shortcut. Lenders that issue "qualified mortgages" (QMs) are *presumed* to comply with the ATR rule. To qualify, loans must:

- Not include excessive points and fees (generally, no more than 3% of the loan amount, with certain exceptions),
- Not include risky features, such as interest-only provisions, negative amortization or terms longer than 30 years,
- Be made to borrowers with DTIs of 43% or less (with an exception for small portfolio lenders and a temporary exception for loans that meet the underwriting requirements of Fannie Mae, Freddie Mac or certain other government-sponsored enterprises), and
- Not include balloon payments (with an exception for smaller creditors in rural or underserved areas).

As discussed below, these requirements are relaxed for community banks.

The level of protection the QM rule provides depends on the interest rate. If it exceeds the average prime rate by less than 1.5%, the QM rule provides a *safe harbor*. So long as a loan is a QM, it's deemed to satisfy the ATR rule.

But for higher-priced loans — those with interest rates that exceed the average prime offer rate, also known as the APOR, by 1.5% or more — a lender receives only a *rebuttable presumption* of compliance. In other words, even if the loan is a QM, the lender can be liable for violating the ATR rule if the borrower proves that the lender failed to make a reasonable, good-faith determination of the borrower's ability to repay.

Relief for community banks

The new rules place many community banks in a difficult position. They must strike a balance between 1) protecting themselves from liability and penalties by making QMs, and 2) making loans that serve the needs of their communities.

In July, the CFPB amended the rules to provide some relief for "small creditors" — those with assets of $2 billion or less and that make no more than 500 first-lien mortgages per year. For these lenders, loans held in their portfolios for at least three years will be considered QMs even if a borrower's DTI exceeds 43%, so long as they otherwise meet the QM requirements.

The amendments also increase the interest-rate threshold from 1.5% to 3.5%. Thus, a small lender that charges less than 3.5% over the APOR can still qualify for the safe harbor. And, during a two-year transition period, small lenders can make QMs with balloon payments, even if they're not in rural or underserved areas.

Review the requirements

In addition to the ATR and QM rules, several other mortgage-related rules will take effect on Jan. 1, 2014. They include new mortgage servicing rules — covering topics such as periodic billing statements and interest-rate adjustment notices, enhanced appraisal requirements for certain loans, and new restrictions on loan originator compensation.

All community banks should review their loan portfolios, policies, procedures and documentation and develop plans for implementing the new rules. ▲

BANK
Wire

BASEL III FINALIZED

In July, the OCC and the Federal Reserve Board approved final rules — and the FDIC approved an identical "interim final rule" — adopting Basel III bank capital requirements.

The rules establish a 4.5% minimum ratio of common equity tier 1 capital to risk-weighted assets and a common equity tier 1 capital conservation buffer of 2.5% of risk-weighted assets. They also increase the minimum ratio of tier 1 capital to risk-weighted assets from 4% to 6% and set a minimum leverage ratio of 4%.

The final rules contain several changes from the proposed rules designed to reduce the rules' impact on smaller banks. For example, they retain the current risk-weighting approach for residential mortgages and, for banks with total assets of $250 billion or less, provide an opt-out from regulatory capital recognition of accumulated other comprehensive income.

The rules also "grandfather" the eligibility of trust-preferred securities to qualify as tier 1 capital for smaller bank holding companies (those with less than $15 billion in total consolidated assets). Banks with more than $250 billion in total assets must comply with the new rules beginning Jan. 1, 2014. Other banks have until Jan. 1, 2015. ▲

OCC PUBLISHES COMMUNITY BANKING GUIDE

The OCC in June published *A Common Sense Approach to Community Banking*. The booklet emphasizes best practices in three areas:

- Risk assessment and management,
- Strategic planning, and
- Capital planning.

The booklet provides community banks with welcome practical advice, as well as insights into what federal regulators are looking for. It can be downloaded at occ.gov. (Click on "publications.") ▲

FTC PUBLISHES RED FLAGS "HOW TO"

The Federal Trade Commission's (FTC's) Red Flags Rule requires financial institutions and certain other creditors to develop, implement and administer a written identity theft prevention program. The FTC recently published *Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business*. The guide outlines a four-step compliance process and answers frequently asked questions about the rule. You can find it at business.ftc.gov. (Click on "Red Flags Rule" under "Privacy & Security.") ▲

LESSONS FROM RESILIENT BANKS

A recent study by the St. Louis Federal Reserve Bank identifies the distinguishing features of community banks that maintained the highest supervisory ratings during the recent financial crisis (2006 to 2011). The authors identify balance sheet and income-statement ratios that separated thriving banks from the pack and supplement their analysis with detailed interview evidence. You can find the report — *The Future of Community Banks: Lessons from Banks That Thrived During the Recent Financial Crisis* — at research.stlouisfed.org. (Type "9833" in the search box.) ▲

P&G Associates

P&G Associates ("P&G") has been meeting the specific risk management needs of community banks of all sizes since 1991. As a high quality and affordable alternative to national firms, P&G provides internal audit, regulatory compliance, BSA/AML, information technology and enterprise risk management review services and software. P&G is exclusively dedicated to the banking industry, providing clients with dedicated, focused and hand-held services reflective of a wide range of skills, experience and industry expertise. As a Firm, we have also been proactive in assisting our clients with the designing, implementation and testing of the internal control environment to assist management with the attestation requirement under the Sarbanes-Oxley Act.

P&G's uniqueness is characterized by its experienced staff and partners. Their hands-on involvement on each engagement provides our clients with a wide range of skills, experience and industry expertise. We employ the use of Subject Matter Experts — designated individuals performing audits in their specific field of expertise. The use of such professionals provides a unique value-added approach that is both efficient and productive.

We believe that a significant aspect of our services is our degree of involvement and responsibility to assist management by making suggestions for improvement, keeping them informed of professional developments and by acting as an independent counsel and sounding board on general business matters and new ideas.

We pride ourselves in our ability to provide effective and practical solutions that are commensurate with our clients' needs by emphasizing high-quality personalized service and attention. Our services are truly customized.

For **Solutions** *to your internal audit needs, please contact our service coordinators at (877) 651-1700, or log-on to www.pandgassociates.com to learn more.*

P&G Associates

www.pandgassociates.com

Headquarters:
646 US Highway 18
East Brunswick, NJ 08816

Offices:
New York, NY
Philadelphia, PA
Chicago, IL
Miami, FL