P&G Banking

ADVISOR

Summer 2014

Weighing in on your borrowers' working capital levels

Avoid these common holding-company reporting errors

BANK *Wire*

Is your bank on top of cybersecurity?

2 severe threats loom over financial institutions

P&G Associates

www.pandgassociates.com 877.651.1700

Is your bank on top of cybersecurity?

2 severe threats loom over financial institutions

Mitigating the risks associated with cyberattacks is among the most potent challenges banks face today. Increasing use of online and mobile banking technologies has made banks and their customers more vulnerable than ever before. Given the huge cost of a data breach — in terms of both monetary loss and reputational damage — all banks should have a solid program for assessing and addressing cybersecurity risks.

Over the last decade, bank regulators — through the Federal Financial Institutions Examination Council (FFIEC) — have issued guidance on several aspects of cybersecurity. Most recently, the FFIEC outlined the steps banks should take to address two severe threats: 1) distributed denial-of-service (DDoS) attacks and 2) cyberattacks on ATM and card authorization systems.

Combating DDoS

In a recent statement, the FFIEC alerted banks to the risks associated with DDoS attacks on public websites. These attacks slow website response times and otherwise disrupt network resources. They're designed to prevent customers from accessing bank information and services and to interfere with back-office operations.

Regulators expect banks to address DDoS readiness as part of their ongoing information security and incident response plans.

In some cases, the FFIEC explained, criminals use DDoS attacks as a diversionary tactic in connection with attempts to initiate fraudulent wire or ACH transfers using stolen customer or bank employee credentials.

Regulators expect banks to address DDoS readiness as part of their ongoing information security and incident

response plans. In addition to evaluating the risks to critical systems, banks should:

- Monitor website traffic to detect attacks,
- Activate incident response plans as appropriate (including notification of Internet service providers and customers), and
- Consider sharing information with law enforcement and organizations such as the Financial Services Information Sharing and Analysis Center (FS-ISAC).

Banks also should ensure sufficient staffing for the duration of an attack and consider engaging third-party service providers to manage Internet traffic flow. Following an attack, a bank must identify any gaps in its response and modify its risk management controls accordingly.

The statement lists several resources available to help banks mitigate the risks of DDoS attacks, including the Department of Homeland Security's *DDoS Quick Guide*, available at us-cert.gov. (Click on "Publications" and "DDoS Quick Guide.")

Defending against ATM attacks

The FFIEC also has warned about a dangerous form of ATM cash-out fraud known as "unlimited operations." It enables criminals to withdraw funds well beyond ATM control limits and even beyond the cash balance

in customer accounts. In one recent attack, criminals used unlimited operations to steal more than $40 million using only 12 debit card accounts.

To perpetrate this scheme, criminals typically send phishing e-mails to bank employees in an attempt to install malware on the bank's network, giving themselves the ability to alter the settings on Web-based ATM control panels. By increasing or eliminating limits on ATM cash disbursements and reducing fraud and security-related controls, criminals can quickly withdraw significant sums using fraudulent debit or other ATM cards.

The statement notes that banks may initially be liable for ATM fraud losses, even if they outsource their card issuing function to a card processor and the compromise takes place at the processor.

To mitigate ATM fraud risks, banks should:

- Conduct ongoing information security risk assessments,
- Perform security monitoring, prevention and risk mitigation, including monitoring third-party processors and ATM transaction activity for unusual behavior,
- Take steps to protect against unauthorized access,
- Review — and periodically test — the adequacy of controls over IT networks, card authorization systems, ATM usage parameters and fraud detection processes,
- Conduct regular training programs,
- Test incident response plans, and
- Participate in industry information-sharing programs, such as FS-ISAC.

Regulators expect banks to incorporate ATM fraud risks into their regular risk management processes, consistent with the *FFIEC Information Technology Examination Handbook*. And banks that create PINs for cardholders must follow the *Payment Card Industry (PCI) PIN Security Requirements*.

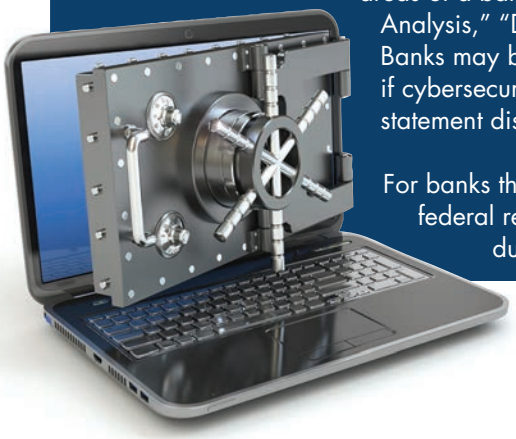
Assess your risk

As technology continues to advance and fraud schemes become more sophisticated, it's critical for banks to evaluate their risks on an ongoing basis. The FFIEC urges banks to revisit their risk assessments at least once a year — more frequently if they introduce new electronic services or receive new information about potential risks or vulnerabilities. ▲

Cybersecurity: Keeping shareholders informed

Many banks struggle with the appropriate level of disclosure regarding cybersecurity risks and incidents. Unfortunately, there's relatively little guidance on this subject from banking regulators. Regulators expect banks to notify customers when they become aware of unauthorized access to customer information and determine that misuse of the information has happened or is reasonably possible. But what about disclosure to shareholders?

Banks that file reports with the SEC may be required to disclose cybersecurity risks and incidents in their filings. Under SEC guidance, depending on the level of risk involved, disclosure may be appropriate in one or more areas of a bank's reports, including "Risk Factors," "Management's Discussion and Analysis," "Description of Business," and "Disclosure Controls and Procedures." Banks may be required to disclose legal proceedings involving cyber incidents and, if cybersecurity risks or incidents result in material costs or losses, to make financial statement disclosures.



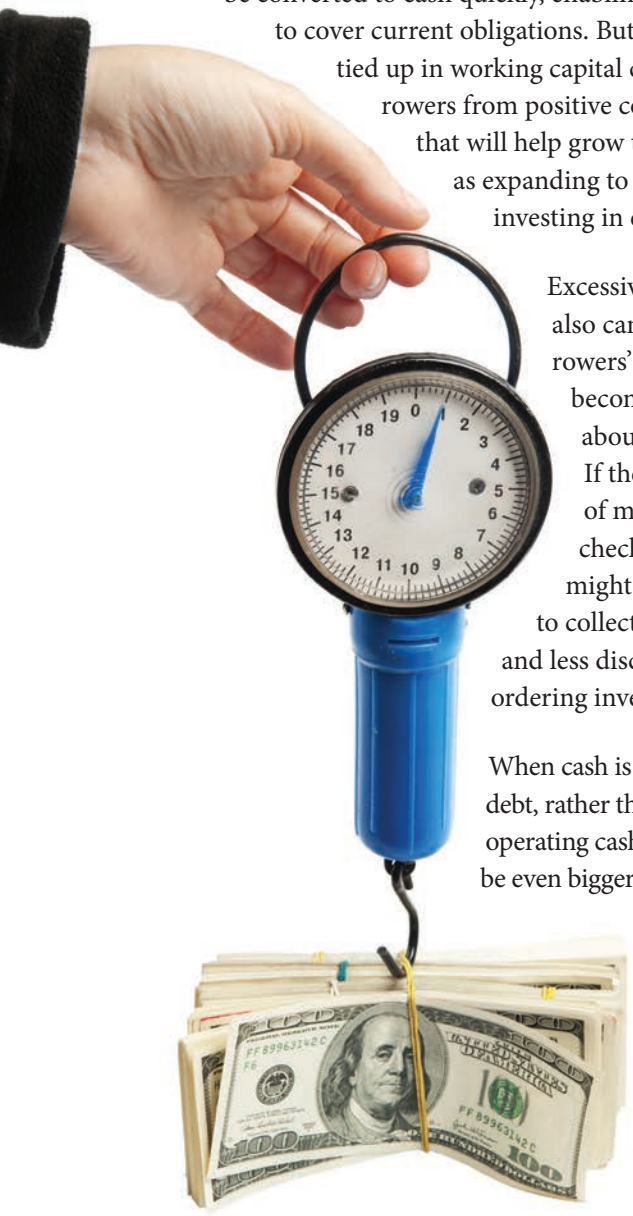
For banks that don't file with the SEC, there's no explicit disclosure guidance from federal regulators. Nevertheless, it's a good idea to develop policies and procedures for disclosing cybersecurity risks and incidents to shareholders.

Weighing in on your borrowers' working capital levels

A pet phrase in the financial arena is "Capital is king." But is this a case where there can be too much of a good thing? If so, how should you communicate this to your borrowers?

Enough vs. too much

An ample amount of working capital allows assets to be converted to cash quickly, enabling your borrowers to cover current obligations. But too much cash tied up in working capital can prevent borrowers from positive courses of action that will help grow the business, such as expanding to new markets or investing in equipment.



Excessive cash balances also can encourage borrowers' management to become complacent about working capital. If they have plenty of money in the checkbook, they might be less hungry to collect receivables and less disciplined when ordering inventory.

When cash is generated through debt, rather than improved operating cash flow, there could be even bigger problems. In such situations, borrowers need to earn a higher return on their investments than they're paying in interest. But those that employ sloppy working capital practices are unlikely to achieve adequate returns. Eventually, debt and interest payments can overwhelm borrowers.

> Thanks to reduced interest rates on new debt and higher revenues, some borrowers are stockpiling cash.

Thanks to reduced interest rates on new debt and higher revenues, some borrowers are stockpiling cash. You might notice that a borrower's working capital has increased over the last few years or is significantly higher than that of its competitors. Proactive lenders point out the trend and encourage effective collections and inventory management strategies.

Collections must be timely

When a borrower sells on credit, it finances its customers' operations. Stale receivables — typically any balance over 45 or 60 days outstanding, depending on the industry — are a red flag.

Getting a handle on receivables starts by honestly evaluating which items should be written off as bad debts. Then viable balances need to be "talked in the door" as soon as possible. Enhanced collections efforts might include early bird discounts, electronic invoices and collections-based sales compensation programs.

Dedicated collections staff should be charged with approving and monitoring customer credit, sending out collections letters, and making phone calls for any invoices more than 30 days late. Consequently, they should be among your borrowers' most dedicated employees.

Alternatively, some borrowers sell or "factor" receivables to a third party at a discount, typically 20% to 30% off the invoice amount.

Inventory: Data and technology help

Inventory is a huge investment for manufacturers, distributors, retailers and contractors. It's also difficult to track and value. Enhanced forecasting and data sharing with suppliers can reduce the need for safety stock and result in smarter ordering practices.

Computerized technology — such as barcodes, radio frequency identification and enterprise resource planning tools — also improves inventory tracking and ordering practices. These solutions often come with a hefty price tag, but not always.

Handheld replenishment devices are a simple solution manufacturers use to improve line productivity and lower their investment in work-in-progress inventory. Here, line workers press replenishment buttons on wireless devices when they need more materials at their station. This signals a refill request to the forklift driver, who then immediately replenishes the worker's supply.

Keeping an eye on it

While collections and inventory are significant factors when it comes to working capital management, accounts payable can't be ignored. Borrowers should never pay a bill the day it's received. Instead, they should extend terms as long as possible — without losing out on any early bird discounts.

Typically borrowers with the most effective working capital management practices will be the lowest credit risk. Encourage your borrowers to manage their working capital levels wisely, and scrutinize working capital when making new loans. ▲

Avoid these common holding-company reporting errors

Small bank holding companies — those with less than $500 million in total consolidated assets — are required to file semiannual FR Y-9SP reports with the Federal Reserve Board (FRB) as of the last calendar day of June and the last calendar day of December. The FRB uses information in these reports to monitor and analyze a holding company's financial condition, spot potential financial trends or problems and review merger and acquisition applications.

In a recent paper, FRB staff outlined common errors made on holding companies' FR Y-9SP reports.

Reconciliation with call reports

Assuming that a holding company owns 100% of a bank subsidiary's equity, common errors made on call reports include the following:

- The holding company's dividend income on the FR Y-9SP doesn't equal the bank subsidiary's dividend payments.
- The holding company's equity in the bank's undistributed income or loss on the FR Y-9SP doesn't equal the bank subsidiary's net income less its dividends declared or paid.

- The holding company's equity investment in bank subsidiaries and associated banks on the FR Y-9SP doesn't equal the bank subsidiaries' total equity capital.
- The holding company's total consolidated assets on the FR Y-9SP are less than the bank subsidiary's total assets.

If the holding company owns less than 100% of the subsidiary's equity, a pro-rata calculation is necessary to reconcile these items.

Reconciliation with structure reports

The FRB cross-checks certain line items from the FR Y-9SP with the FR Y-6 (*Annual Report of Bank Holding Companies*) and FR Y-10 (*Report of Changes in Organizational Structure*) "structure reports." Common errors include the following:

- There's a discrepancy between the holding company's equity investment in a bank subsidiary, which is calculated based on 100% ownership, and the holding company's most recent FR Y-6, which indicates less than 100% ownership. This could indicate an error in the FR Y-6 or a need to file an FR Y-10 to report a change in ownership.
- Structure data regarding nonbanking companies or activities doesn't coincide with FR Y-9SP report data.

Other errors

The FRB's paper lists several other common reporting errors made by bank holding companies. Examples include the following:

- Cash dividends reported in the FR Y-9SP don't include dividends from both common and preferred stock.
- FR Y-9SP, Schedule SC-M, No. 14, isn't completed. This section asks whether all changes in investments and activities have been reported on an FR Y-10 and also asks for the name and phone number of the holding company official verifying FR Y-10 reporting.

Many holding companies omit external audit information from the FR Y-9SP.

Many holding companies also omit external audit information from the FR Y-9SP. The form requires holding companies to state whether or not they have "engaged in a full-scope external audit at any time during the calendar year" and, if the answer is "yes," to provide the name and address of the external auditing firm. This section should be left blank in the June filing but should be completed in the December filing.

Are your reports accurate?

It's in a bank holding company's best interest to ensure that its Federal Reserve reports are accurate. In addition to minimizing the time and expense of corrections and follow-up, completing the forms correctly ensures that the data, which is made available to the public, is reliable. ▲

BANK
Wire

CFPB TO EXPAND HMDA REPORTING

The Consumer Financial Protection Bureau (CFPB) is considering changes to improve and expand data collection under the Home Mortgage Disclosure Act (HMDA). Currently, lenders are required to report the type and general location of the property; the race, ethnicity and sex of the applicant; the amount of the loan; and the purpose of the loan (purchase, refinance or home improvement).

The Dodd-Frank Act directed the CFPB to expand HMDA reporting to include total points, fees and rate spreads for all loans; riskier loan features, such as teaser rates, prepayment penalties and nonamortizing features; lender information, including a unique identifier for the loan officer and the loan; property value and improved property location information; and the applicant's age and credit score.

The CFPB is considering additional reporting requirements, including:

- Mandatory reporting of denial reasons,
- Debt-to-income ratios,
- Qualified mortgage status (under the CFPB's ability-to-repay rule),
- Combined loan-to-value ratios,
- Automatic underwriting system results,
- Additional details about points and fees (including total origination charges; total discount points; risk-adjusted, prediscounted interest rates; and interest rates), and
- Affordable housing restrictions and manufactured-housing data.

Collecting and submitting this information could be burdensome for lenders. So the CFPB is seeking feedback on ways it can streamline reporting, improve data entry and standardize the reporting threshold — for example, by requiring banks to report only if they make 25 or more loans per year and meet certain other conditions. ▲

BANKS PLACE HIGH AMONG OCCUPATIONAL FRAUD VICTIMS

In combating fraud, banks tend to focus on external threats. But occupational fraud — fraud involving abuse of trust by employees and other insiders — is an enormous problem. According to the Association of Certified Fraud Examiners' 2012 *Report to the Nations on Occupational Fraud and Abuse*, the typical organization loses 5% of its revenues to fraud each year, and banking and financial services is the most commonly victimized industry.

The most common fraud schemes in the banking and financial services industry are corruption (bribery, conflicts of interest and other abuses of an employee's influence over a business transaction) and misappropriation of cash on hand. The median loss is $232,000. ▲

BAD ACTOR? NO BANK FOR YOU!

The FDIC has adopted a final rule prohibiting certain "bad actors" from buying failed banks — or assets of any covered financial company — from the FDIC. Under the rule, which implements a section of the Dodd-Frank Act, bad actors include individuals or entities that have, or may have, contributed to a covered financial company's failure. ▲

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