# P&G Banking ADVISOR

Winter 2017




P&G Associates

www.pandgassociates.com 877.651.1700

# CYBERSECURITY TAKES THE SPOTLIGHT

Cybersecurity is a key issue for banks today, so it's no surprise that federal and state regulators have been scrutinizing banks' information security (IS) efforts. Recently, several federal and state regulatory agencies have taken some new steps in the ongoing effort to protect sensitive account information. In light of the heightened scrutiny — and the significant risks involved — it's a good idea for all banks to review and, if necessary, update their cybersecurity programs.

## RECENT DEVELOPMENTS

In September 2016, the Federal Financial Institutions Examination Council (FFIEC) updated its *Information Security* booklet, part of its *Information Technology Examination Handbook*. The booklet provides banks with an excellent framework for evaluating and strengthening their cybersecurity programs.

Also in September, the New York State Department of Financial Services proposed comprehensive cybersecurity requirements for banks and other financial institutions. (See "State regulation of cybersecurity: A burgeoning trend?" on page 3.)

Finally, in October 2016, the OCC, FDIC and Federal Reserve issued a joint proposal to develop enhanced cyber risk management standards for the largest financial institutions (those with total consolidated assets of $50 billion or more).

## WHAT EXAMINERS LOOK FOR

According to the FFIEC booklet, an effective IS program should cover four key areas: 1) risk identification, 2) risk measurement, 3) risk mitigation, and 4) risk monitoring and reporting. The 95-page publication contains detailed guidance on identifying threats, measuring risk, defining IS requirements and implementing appropriate controls.

An appendix contains updated examination procedures, providing valuable insights into examiners' cybersecurity expectations. The procedures are designed to meet a number of examination objectives, including determining whether management:

- Promotes effective governance of the IS program through a strong IS culture, defined responsibilities and accountability, and adequate resources,
- Has designed and implemented the program so that it supports the bank's IT risk management process, integrates with its lines of business and support functions, and is responsive to the cybersecurity concerns associated with the activities of technology service providers and other third parties,
- Has established risk identification processes,
- Measures risk to help guide the development of mitigating controls,
- Effectively implements controls to mitigate identified risk, and
- Has effective risk monitoring and reporting processes.

In addition, it's important to ascertain whether security operations encompass necessary security-related functions, are guided by defined processes, are integrated with lines of business and activities outsourced to third-party service providers, and have adequate resources. Implementing assurance and testing activities to provide confidence that the program is operating as expected and reaching its goals is also necessary.

Although the guidance applies to all types of institutions, the booklet emphasizes that banks should develop and maintain risk-based IS programs commensurate with their size and operational complexity.

## FOCUS ON SECURITY OPERATIONS

The updated publication contains a new section on security operations that emphasizes:

**Threat identification.** A bank should go beyond risk identification to pinpoint specific threat sources and vulnerabilities and analyze the potential for exploitation. Management can use this information to develop strategies and tactics for protecting the bank's IT system and detecting attacks.

**Threat monitoring.** Threat monitoring — both continual and *ad hoc* — is critical. And management should clearly delineate the responsibilities of security personnel and system administrators as well as review and approve monitoring tools and the conditions under which they're used. Monitoring should focus not only on incoming network traffic, but also on outgoing traffic to identify malicious activity and data exfiltration.

**Incident identification and assessment.** Management needs a process that will identify compromise indicators — for example, antivirus alerts or unexpected file changes or logins — and rapidly report them for investigation.

**Incident response.** A bank's incident response plan should include defined protocols for containing an incident, coordinating with law enforcement and third parties, restoring systems, preserving data and evidence, and providing customer assistance.

## THIRD-PARTY OVERSIGHT

Banks often outsource services, such as data and transaction processing, cloud computing and even information security. But management remains responsible for ensuring the bank's system and information security.

Oversight of outsourced activities includes due diligence in selecting and managing third-party service providers. In addition, management should obtain contractual assurances for security, controls and reporting; get nondisclosure agreements regarding the bank's data and systems; and arrange for independent auditing and testing of third-party security.

## GET WITH THE PROGRAM

Given the level of regulatory activity related to cybersecurity and the serious consequences of a data breach, banks can expect scrutiny of IS programs to intensify. Now's the time to review your program to ensure that your institution is protected. ■

## STATE REGULATION OF CYBERSECURITY: A BURGEONING TREND?

In September 2016, the New York State Department of Financial Services (DFS) proposed comprehensive cybersecurity requirements for banks and other financial institutions under its jurisdiction. Among other things, the proposal would require banks to undertake the following steps:

- Establish and maintain a cybersecurity program — reviewed by the board of directors and approved by a senior officer — designed to ensure the confidentiality, integrity and availability of its information systems.
- Incorporate certain mandatory functions into the program, designed to identify risks, implement defensive infrastructure and policies, detect and respond to cybersecurity events, and fulfill regulatory reporting obligations.
- Appoint a chief information security officer with specified responsibilities, including providing the board with biannual written assessments of the program.
- Adopt written cybersecurity and third-party information security policies addressing specified areas.
- File annual certifications of compliance with the DFS and report material cybersecurity events to the agency within 72 hours.

If finalized, the proposed regulations likely would affect not only New York banks, but also banks that do business in New York. This also could mark the beginning of a trend toward increased state regulation of cybersecurity.

# NEW RULES ON CUSTOMER DUE DILIGENCE

## FinCEN answers frequently asked questions about beneficial ownership

Beginning on May 11, 2018, financial institutions will be required to verify the identities of the beneficial owners of their legal-entity customers when those entities open new accounts. This is the result of an action in May 2016 by the Financial Crimes Enforcement Network (FinCEN), which issued its "Customer Due Diligence Requirements for Financial Institutions" (CDD Rule).

More recently, FinCEN published frequently asked questions (FAQs) to help banks understand the new requirements and incorporate them into their Bank Secrecy Act and anti–money-laundering (BSA/AML) compliance programs.

### THE HIGHLIGHTS

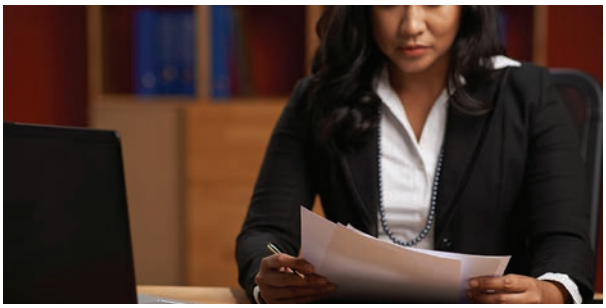
Here's a brief look at some of the often-asked questions and responses about the new requirements:

**Q:** Which institutions are covered?

**A:** The CDD Rule applies to federally regulated banks and federally insured credit unions, as well as to mutual funds, securities brokers and dealers, and certain other financial services firms. Note that a recent FinCEN proposal would expand its customer identification program (CIP) requirements, including the CDD Rule, to non–federally regulated institutions.

**Q:** What's a legal-entity customer?

**A:** Generally, "legal entity" refers to a corporation, limited liability company or general partnership, or similar entities formed in foreign jurisdictions. It also includes limited partnerships, business trusts and other entities created by filing a public document with the Secretary of State or its equivalent. Exceptions include natural persons, unincorporated associations, government entities,



federally regulated financial institutions and U.S. public companies.

**Q:** Which accounts are covered?

**A:** The CDD Rule generally uses the same definition of "account" as the CIP rules do, with certain exceptions. Covered institutions are required to obtain beneficial owner information only for *new* accounts opened on or after May 11, 2018. The rule doesn't apply to existing accounts.

**Q:** Who's a beneficial owner?

**A:** There are two types of beneficial owners:

1. Each individual, if any, who owns 25% or more of an entity's equity interests (directly or indirectly — the "ownership prong"), or

2. A *single* individual — such as a CEO, CFO, COO, president, vice president, treasurer, managing member, general partner or other person who performs similar functions — with significant responsibility to control, manage or direct an entity (the "control prong").

Generally, covered financial institutions are required to collect beneficial ownership information concerning

up to five individuals for a given legal-entity customer: one person under the control prong, and zero to four persons under the ownership prong.

### REQUIRED PROCEDURES

Covered institutions must establish and maintain written procedures that are "reasonably designed to identify and verify the beneficial owners of legal-entity customers" at the time a new account is opened. These procedures should, at a minimum, contain the same elements the CIP rules require for verifying individual customer identities. But the regulator's FAQs clarify that, for documentary verification, institutions may use photocopies or other reproductions of identification documents.

Institutions needn't obtain information *directly* from an entity's beneficial owners. Rather, they may obtain such information from the individual seeking to open a new account on behalf of the legal entity.

The CDD Rule also amends the BSA/AML requirements to require covered institutions to implement and maintain appropriate risk-based procedures for conducting *ongoing* customer due diligence.

### GET READY

If your bank is covered by the CDD Rule, you have until May 11, 2018, to comply. Because examiners may ask you about your preparation process if they visit you before the effective date, begin now to review your BSA/AML program and be sure you have a plan to ensure the policies and procedures are in place to collect information about the beneficial owners of legal-entity customers. ■

# DON'T COMPARE APPLES TO ORANGES

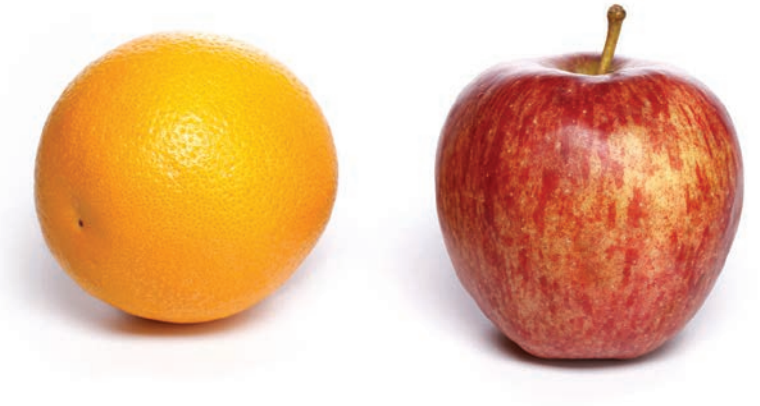
## Evaluate borrowers accurately by normalizing financial statements

In evaluating their borrowers, lenders need to use all the tools at their disposal — including an accounting tactic called "normalizing." Normalizing involves adjustments to income statements and balance sheets to compensate for companies' differing accounting methods. Because borrowers' accounting practices vary widely, comparing them without adjusting their financial statements is like comparing apples to oranges. Ultimately, failing to normalize financial statements may result in faulty lending decisions.

### NO TWO ARE ALIKE

Even within the broad confines of Generally Accepted Accounting Principles (GAAP), it's rare for two companies to follow exactly the same accounting practices. When you compare a borrower's practices to those of a competitor or to industry benchmarks, it's important to understand how they report transactions.

A small firm, for example, might report earnings when cash is received (cash basis accounting), but its competitor might record a sale when it sends out



the invoice (accrual basis accounting). Differences in inventory reporting, pension reserves, depreciation methods and cost capitalization vs. expensing policies also are common.

> ONE-TIME CHARGES — INSURANCE CLAIMS AND FRAUD LOSSES ARE EXAMPLES — COULD SHED LIGHT ON FUTURE RISK FACTORS.

Additionally, some tax accounting practices — expanded Section 179 and bonus depreciation deductions, for example — may temporarily defer income taxes. So, consider the tax implications when reconciling different tax accounting methods.

## PAST VS. FUTURE

Lenders need to distinguish between historic performance results that represent potential ongoing earning power and those historic results that don't. If a one-time revenue (or expense) or gain (or loss) will temporarily distort the company's future earnings potential, you would add back expenses and losses (or subtract the revenues and gains) if they're not expected to recur.

If a borrower's plant was devastated by a hurricane or a borrower experienced a $1 million equipment theft, for instance, you'd add back the extraordinary losses to get a clearer picture of normal operating performance. Or if the borrower won a $5 million lawsuit, you'd subtract the gain. Other nonrecurring items might include discontinued lines or expenses incurred in an acquisition.

But go beyond just adjusting these charges. One-time charges — insurance claims and fraud losses are examples — could shed light on future risk factors. Ask about the nature of these charges and any preventive measures the borrower has taken or will be taking to minimize the risk of recurrence.

## AT ARM'S LENGTH

Some closely held business owners are paid based on the company's cash flow or the owner's personal needs, not on the market value of services they provide. Many closely held businesses also employ family members, conduct business with affiliates and extend loans to company insiders.

Because of this, you, as the lender, should identify all related-party transactions and inquire whether they occur at "arm's length." Also consider reconciling for unusual perquisites provided to insiders, such as season tickets to sporting events, college tuition or company vehicles.

## ON AN EQUAL BASIS

While most normalizing reconciliations are made to the income statement, many flow through to the balance sheet, which is often the lender's starting point in determining collateral values.

Suppose one manufacturer uses eight-year useful lives for its equipment, but another uses six-year useful lives for the same items. To create an equal basis of comparison, you might reconcile the first company's earnings downward to reflect its slower depreciation technique. In addition, the net book value of its equipment should be lowered to reflect its relatively inadequate depreciation deductions. These lender-made normalizing adjustments effectively make the first borrower appear less attractive than initially shown on its financial statements when compared to the second borrower.

## SEE YOUR BORROWERS AS THEY ARE

Obviously, you need to evaluate each borrower based on its individual circumstances. But in assessing your borrowers' performances and potential for future growth, you also need to be able to engage in comparisons — whether between industries or over time. To that end, normalizing reconciliations to financial statements can help you see borrowers' financial situations more clearly, leading to better lending decisions. ■

# BANK WIRE

## BEWARE OF UDAAP

The Consumer Financial Protection Bureau (CFPB) continues to exercise its authority to crack down on banking practices it views as unlawful under the Dodd-Frank Act's regulations on unfair, deceptive or abusive acts or practices (UDAAP). In one recent enforcement action, for example, the agency entered into a $28.5 million settlement with the Navy Federal Credit Union for alleged UDAAP violations related to its collection of delinquent accounts.

The institution's unfair, deceptive or abusive practices included:

- Threatening legal action it didn't intend to take or lacked the authority to take, including wage garnishment,
- Making false threats to contact service members' commanding officers (the CFPB found that an account agreement provision permitting the credit union to do so wasn't consented to, as required, because the clause was "buried in fine print, non-negotiable and not bargained for by consumers"), and
- Misrepresenting the impact of loan delinquencies on customers' credit ratings.

The institution also unfairly froze customers' electronic account access and disabled some electronic services after the accounts became delinquent. ■

## OCC GUIDANCE ON CORPORATE AND RISK GOVERNANCE

Recently, the OCC revised its *Corporate and Risk Governance* booklet, which is part of its *Comptroller's Handbook*. Among other things, the updated booklet:

- Outlines management and board responsibilities for governing a bank's structure, operations and risks,
- Explains enterprise risk management (ERM) and the importance of viewing risk in a comprehensive, integrated manner,
- Discusses the benefits of a risk governance framework — and the role of risk culture and risk appetite within that framework, and
- Provides guidance on strategic, capital and operational planning.

You can find the booklet at occ.gov, under "Publications." Click on *Comptroller's Handbook*. ■

## SHOULD YOUR BANK HAVE A FRAUD HOTLINE?

The evidence suggests that the answer is a resounding "yes" — your bank should have a fraud hotline. Employee fraud is a problem for most organizations, but it's particularly prevalent among banks and other financial institutions. According to the Association of Certified Fraud Examiners (ACFE), banking and financial services was the most-represented sector in its 2016 *Report to the Nations on Occupational Fraud and Abuse*.

According to the report, the most common method of detecting fraud was via tips from employees, customers, vendors and others. In fact, the report found that fraud is more likely to be detected through a tip than as a result of an internal audit or management review. The ACFE also found that organizations with reporting hotlines are nearly twice as likely to detect fraud through tips than those without hotlines.

Telephone hotlines (used by 39.5% of organizations with formal fraud reporting mechanisms) are the most common source of tips, followed by tips submitted via email (34.1%) and tips submitted via Web-based or online forms (23.5%). ■

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