P&G Banking ADVISOR

Fall 2017

THE DANGERS OF ELECTRONIC BANKING
How to manage BSA/AML risks

CAN YOU INCREASE NONINTEREST INCOME?

EDUCATING CUSTOMERS ABOUT CYBERSECURITY

BANK WIRE

P&G Associates

www.pandgassociates.com 877.651.1700

THE DANGERS OF ELECTRONIC BANKING

How to manage BSA/AML risks

Two recent trends are converging to increase banks' risk management obligations. One is heightened scrutiny by banking regulators of their Bank Secrecy Act and Anti-Money Laundering (BSA/AML) compliance efforts. The other is customers' increasing demand for electronic banking (e-banking) services, which can increase a bank's BSA/AML risks.

TAKING A RISK-BASED APPROACH

To help combat money laundering and terrorist financing, banks are called upon to develop and implement comprehensive BSA/AML programs to ensure they know their customers, monitor transactions, identify suspicious activity and share information with the government and other financial institutions. (See "Elements of a BSA/AML program" on page 3.)

Federal regulators emphasize a risk-based approach to BSA/AML compliance. In other words, a bank is expected to conduct a thorough risk assessment and develop policies, procedures and processes that are adequate in light of its size, location, customer base, products and services.

ASSESSING THE IMPACT OF E-BANKING

E-banking — including online account opening, ATM transactions, Internet banking transactions, remote deposit capture (RDC), telephone banking and mobile banking apps — can increase a bank's BSA/AML risks. The lack of face-to-face contact in e-banking transactions introduces a heightened level of risk to institutions by making them vulnerable to unauthorized users accessing customer accounts. As your bank introduces new e-banking products and services, it's imperative to evaluate their impact on your BSA/AML program.

For example, according to the *Federal Financial Institutions Examination Council (FFIEC) BSA/AML Examination Manual*, online account opening without face-to-face contact may heighten your risk because:

- Verifying the customer's identity is more difficult,
- The customer may be outside the bank's targeted geographic area,
- The customer may perceive these transactions as less transparent,
- Transactions are instantaneous, and
- A front company or unknown third party may use the account.

To mitigate these risks, banks should ensure that their BSA/AML monitoring, identification and reporting systems are properly equipped to flag unusual and suspicious activities conducted electronically. Useful tools include ATM activity reports, funds-transfer reports, new-account-activity reports and change-of-Internet-address reports. Reports that identify related or linked accounts are particularly effective in an e-banking context. These reports reveal accounts with common addresses, phone numbers, email addresses and taxpayer identification numbers. Additional risk-mitigating controls may include imposing limits on:

- The types and sizes of transactions that can be conducted through e-banking platforms,
- The volume and frequency of online-initiated transactions (if allowed), and
- Online accounts, to ensure they're offered only to established customers.

The FFIEC emphasizes that, when determining the level of monitoring required for an account, one factor to consider is how the account was opened. Banks need to develop effective and reliable methods for

authenticating a customer's identity when he or she opens an account online (such as "out of wallet" questions that only that person can answer).

MITIGATING RDC RISKS

While RDC provides obvious benefits to customers, it also exposes banks to money laundering, fraud and information security risks. For example, fraudulent, sequentially numbered or physically altered checks may be harder to detect when they're submitted via RDC. Plus, it's difficult for banks to control or locate RDC equipment, particularly when foreign correspondents and foreign money service businesses increasingly rely on RDC.

The FFIEC warns that inadequate controls can result in altered deposit data, duplicate deposits and other problems. Also, customers or service providers typically retain original checks or other deposit items, which may create recordkeeping, data safety and integrity issues.

Potential risk mitigation steps include:

- Performing a comprehensive RDC risk assessment before implementation,
- Conducting appropriate customer due diligence and enhanced due diligence,
- Establishing risk-based parameters for RDC customer suitability, such as lists of acceptable industries and standardized underwriting criteria,
- Comparing an RDC customer's expected account activity to actual activity,
- Establishing RDC transaction limits, and
- Ensuring that RDC customers receive adequate training.

Contracts should clearly set out the relative roles, responsibilities and liabilities of the bank and its customers with respect to RDC transactions, including procedures for handling and disposing of original documents.

ELEMENTS OF A BSA/AML PROGRAM

A bank's BSA/AML program must include, among other things:

- An adequate system of internal controls,
- Appointment of a BSA compliance officer at the management level,
- Ongoing employee training,
- Independent compliance testing,
- A written, risk-based customer identification program (CIP),
- A system for maintaining records of customer information and methods used to verify customer identities,
- Procedures for comparing the customer database and certain transactions against lists of known or suspected terrorists or terrorist organizations maintained by the Office of Foreign Assets Control (OFAC),
- Procedures for filing currency transaction reports (CTRs) for cash transactions that exceed $10,000, as well as for related transactions that exceed $10,000 in the aggregate and transactions that have been structured to avoid reporting, and
- A system for monitoring transactions for suspicious activity and filing suspicious activity reports (SARs) when appropriate.

A comprehensive program can go a long way toward mitigating electronic banking risks.

BEING VIGILANT

The more your bank relies on e-banking products and services, the greater its risks. To avoid compliance issues, be vigilant in monitoring your bank's risk profile and beefing up your BSA/AML program as those risks increase. ■

CAN YOU INCREASE NONINTEREST INCOME?

Although interest income is essential to a community bank's livelihood, it doesn't always meet desired goals. So identifying, and developing, noninterest income sources can make all the difference in your bank's profitability over time. Here are some ways to boost noninterest income.

IDENTIFY THE SOURCES

Common sources of noninterest income include:

- Overdraft and nonsufficient funds charges, which are highly scrutinized, and
- Gains on sales of loans and investment securities.

Noninterest income also may be derived from various products and services — including insurance and annuity products, as well as brokerage, trust and financial planning services.

IMPROVE COLLECTIONS

Community banks have a history of being easy on customers by waiving NSF fees and other penalties anytime they receive complaints. Although it's important for bank personnel to have the discretion to waive these fees, high waiver rates — some estimates are higher than 50% — can quickly wipe out substantial amounts of revenue.

To keep waivers under control, set a target level for discretionary waivers and train bank personnel to understand the significance of noninterest income, make good decisions regarding fee waivers and handle customer complaints. If you haven't already done so, try automating the fee initiation process so that nothing falls through the cracks and incorporate waiver targets into your incentive compensation decisions.

Finally, be sure to include fee waiver data in management reports, which will let you monitor results.

STAY ON TOP OF YOUR MARKET

Banks often miss opportunities to charge higher fees because they fail to keep tabs on their competitors. Identify the predominant banks in your market and procure their fee schedules. Comparing competitors' fees to your own may uncover significant pricing opportunities.

This doesn't mean you should increase your fees to match the highest priced banks in your area; however, if you find your fee schedule is on the low end of the spectrum, a modest increase can have a substantial impact on your bank's revenue. Any change in fee structure should be monitored closely to ensure the strategy produces the desired outcome.

CONSIDER RELATIONSHIP VALUE PRICING

Relationship value pricing can be a highly effective strategy for enhancing fee revenue. It sets prices based on the overall value of a banking relationship with a customer or group of customers, such as a family or a business and its employees.

In its simplest form, relationship value pricing might involve package deals for products or services. A common example is free checking accounts for customers who maintain a minimum loan balance. A more sophisticated approach is to develop customized

pricing based on a valuation of the products and services a specific customer receives.

For relationship value pricing to work, your bank must carefully analyze the costs, benefits and potential profitability of each customer relationship. It's also critical to have systems that monitor the relationship. Banks often lose revenue because they're unaware that the relationship has changed. For example, a bank might continue providing free checking even though the related loan has fallen below the minimum balance or has been paid off.

USE LIFE INSURANCE AS A TOOL

Insurance policies on the lives of directors, officers and other key employees can be cost-effective tools for boosting noninterest income. Your bank can buy coverage or use "split-dollar" arrangements to share the costs and benefits of these policies with employees.

Bank-owned life insurance (BOLI) is often used to fund supplemental executive retirement plans, other nonqualified deferred compensation plans and retiree health benefits. BOLI can be a powerful planning tool because a life insurance policy's cash value grows on a tax-deferred basis and, if the policy is held until the insured employee dies, the death benefit is generally tax-free.

A caveat: To enjoy these tax benefits, your bank must comply with strict notice and consent requirements before buying a policy on an employee's life.

OBTAIN PROFESSIONAL ADVICE

Clearly, to increase your bank's earnings, you need to generate new strategies for developing noninterest income streams. Your financial professional can help you pinpoint specific tactics and determine the best plan for your bank. ■

EDUCATING CUSTOMERS ABOUT CYBERSECURITY

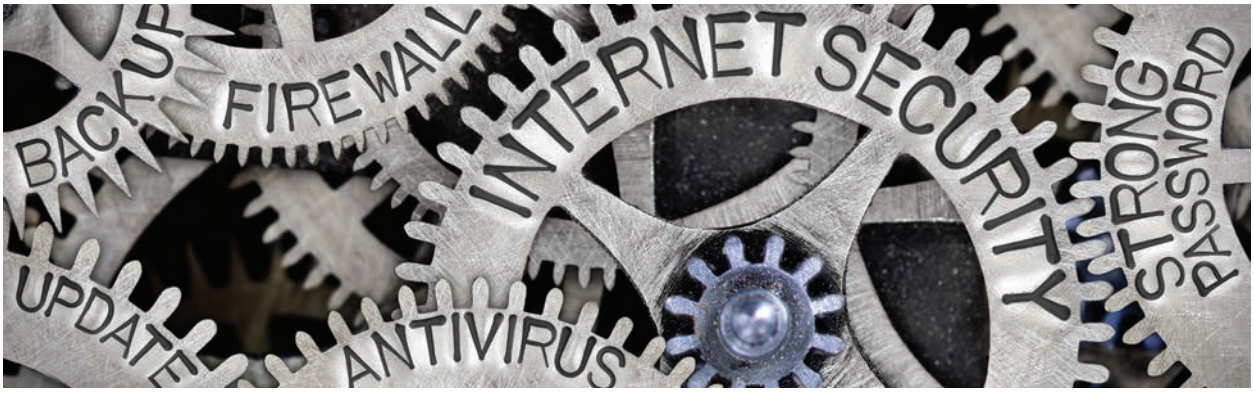
In an increasingly digital world, cybersecurity is one of the biggest issues banks face today. In addition, it's a top priority for federal banking regulators. Many banks have taken steps to assess their cybersecurity risks and implement controls designed to protect their customers' funds and sensitive personal information. But protecting your bank's systems against unauthorized access isn't enough — it's equally important to educate your customers about their role in the process.

LET THEM KNOW THE ISSUES

Here are some issues to address in your customer awareness efforts:

Passwords. No matter how much you invest in cybersecurity controls, your efforts will be for naught if a customer uses an easy-to-detect phrase such as "password1." You can improve security by setting a minimum length and by requiring passwords to include a specific number of special characters. Inform customers about the importance of strong passwords and encourage them to use password management apps, which can help them generate and save more secure passwords.

Multifactor authentication. These days, it's no longer sufficient to rely on one form of customer authentication, such as a password. A better approach is multifactor authentication, or "layered security." One of the most effective tools is "out-of-band" authentication, which requires a transaction initiated through one channel — an online banking app, for example — to be verified through another channel, such as a text message or phone call.



Ideally, multifactor authentication should be mandatory, especially for high-risk transactions. But if it's optional, provide incentives for customers to use it by making them aware of the vulnerability of single-factor authentication, and the effectiveness of multifactor authentication, in protecting their funds and personal information.

Phishing. These schemes are one of the most common and dangerous tools hackers use to compromise bank customers' accounts. Typically, they involve emails to customers that appear to be from the bank. These emails contain embedded links to impostor websites that trick customers into supplying their login credentials or downloading malware that records everything customers type on their computers.

Today, malware has gotten so sophisticated that some programs can compromise even the most robust online authentication techniques, including some forms of multifactor authentication. So it's even more important to educate customers on how to avoid phishing schemes. Let customers know:

1. The circumstances, if any, under which the bank may contact them on an unsolicited basis,
2. The channels the bank may use to contact them (for example, phone, email or text), and
3. The type of information, if any, the bank may request.

In addition, show customers how to spot phishing emails by looking for poor grammar and punctuation and by hovering the cursor over email addresses or hyperlinks to identify the sender's real address.

Unsecured wi-fi networks. Regardless of the other security measures customers take, their login credentials and other information can be intercepted if they connect to the bank through unsecured wi-fi networks. This can happen if a customer logs onto the bank's website or mobile apps at a coffee house or other public wi-fi hotspot. To avoid this risk, warn your customers not to use unsecured networks for banking transactions or, if they must do so, to use virtual private network (VPN) software to establish a secure network connection.

> TODAY, MALWARE HAS GOTTEN SO SOPHISTICATED THAT SOME PROGRAMS CAN COMPROMISE EVEN THE MOST ROBUST ONLINE AUTHENTICATION TECHNIQUES.

ENLIST CUSTOMERS IN THE FIGHT

In the cybercrime wars, ignorance isn't bliss. To enlist customers in the fight against cybercrime, you'll need to let them know about the steps they can take to protect themselves. You can use a variety of vehicles to get the word out, including ad campaigns, social media campaigns, online and mobile banking app alerts, and conversations with bank employees. The important thing is to keep customers informed of their part in the battle. ■

BANK WIRE

IMPACT OF NEW LEASE ACCOUNTING STANDARD ON REGULATORY CAPITAL

Last year, both the Financial Accounting Standards Board (FASB) and the International Accounting Standards Board (IASB) revised their lease accounting standards, effective January 1, 2019, for calendar-year companies. Although there are differences between the FASB and IASB versions, under each standard most leases will be reflected on a lessee's balance sheet as a liability — the obligation to make lease payments — and a related "right of use" (ROU) asset.

How does this affect a bank's regulatory capital in its capacity as lessee? Is the ROU asset included in regulatory capital, like most tangible assets, or deducted from regulatory capital, like most intangible assets? According to the Basel Committee's recent responses to frequently asked questions (FAQs), if the *underlying asset* being leased is a tangible asset, the ROU asset: 1) is included in regulatory capital, 2) is included in the risk-based capital and leverage ratio denominators, and 3) should be risk-weighted at 100%. ■

NEW GOVERNMENT GUIDANCE ON THIRD-PARTY OVERSIGHT

Recently, the Office of the Comptroller of the Currency (OCC) updated its 2013 risk management guidance for third-party relationships. The guidance reaffirms the need for in-depth due diligence and ongoing monitoring of third parties that support critical activities, recognizing that such oversight should be risk based and tailored to each bank's specific needs. Noteworthy in the new guidance are a focus on bank relationships with fintech companies and the ability of banks that use the same third-party service providers to collaborate in meeting the OCC's oversight expectations. For more information, visit occ.gov and type "bulletin 2017-21" in the search box. ■

SETTING UP AN AFFIRMATIVE ACTION PLAN

Federal contractors with 50 or more employees and a single government contract of $50,000 or more are required to maintain a written affirmative action plan (AAP) and meet certain other affirmative action obligations. It may surprise you to learn that financial institutions with 50 or more employees are considered federal contractors if they have accounts insured through the Federal Deposit Insurance Corp. (FDIC) or the National Credit Union Administration (NCUA). ■

CFPB FINALIZES ARBITRATION RULE

Recently, the Consumer Financial Protection Bureau (CFPB), pursuant to its authority under the Dodd-Frank Act, finalized a rule that limits predispute arbitration agreements in certain financial contracts. The CFPB's goal is to provide financial consumers with greater access to class-action lawsuits, a move that's been met with strong opposition by the banking industry. The new rule is set to apply to arbitration agreements entered into on or after March 19, 2018. But stay tuned: There's a movement afoot to repeal the rule through congressional action. ■

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