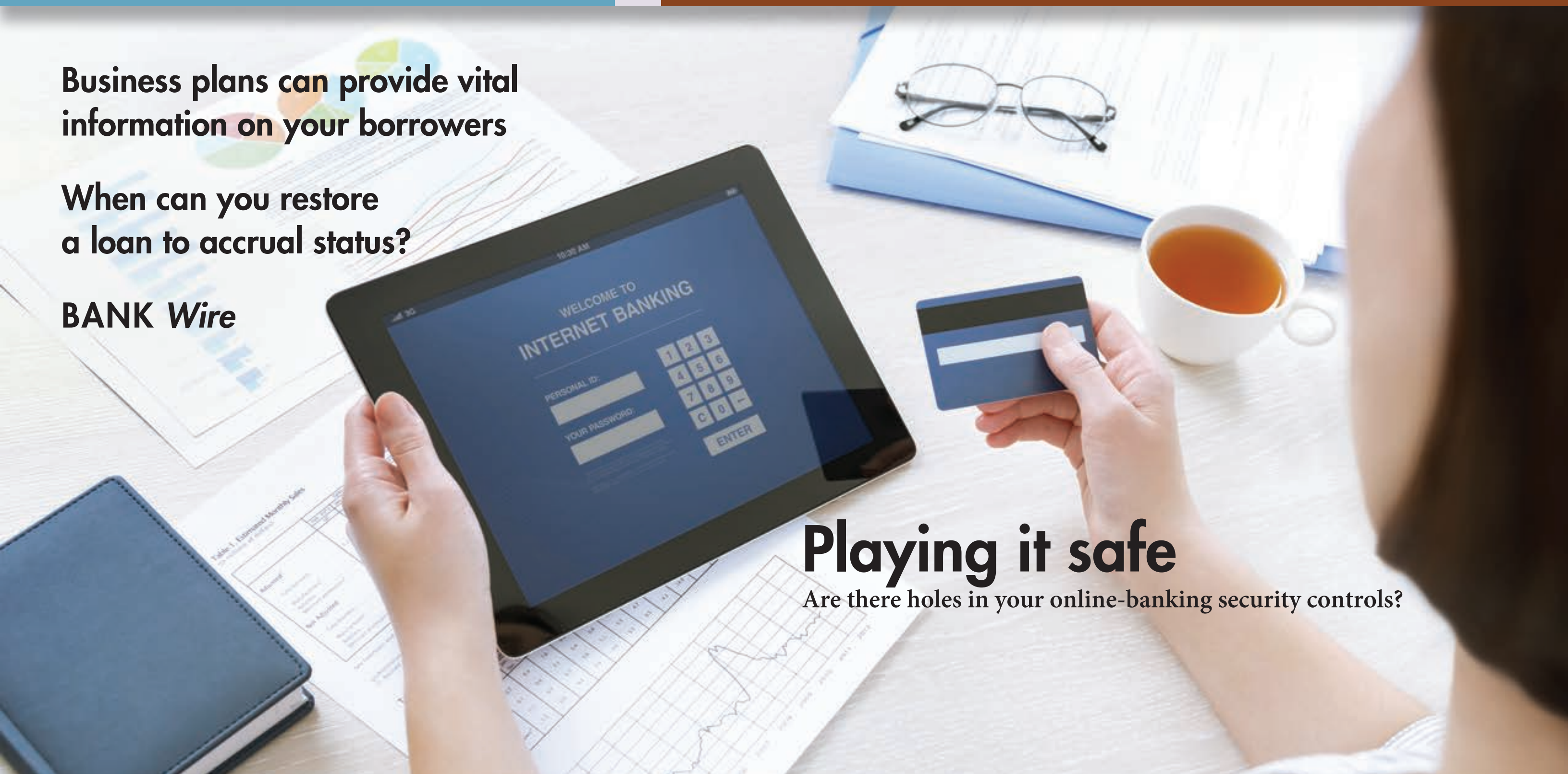
P&G Banking
ADVISOR

Winter 2015



Business plans can provide vital information on your borrowers

When can you restore a loan to accrual status?

BANK *Wire*

Playing it safe

Are there holes in your online-banking security controls?

P&G Associates

www.pandgassociates.com 877.651.1700

Playing it safe

Are there holes in your online-banking security controls?

Online fraud is an enormous problem today, and it's on the rise. But while most banks have taken steps to secure their systems against hackers and other external threats, many remain vulnerable to one of the most common fraud techniques: compromising customers' login credentials to obtain unauthorized access to their online accounts.

For example, a fraudster might send a "phishing" e-mail to customers. The e-mail would contain an embedded link to a phony website, which tricks customers into supplying their login credentials or downloading malware that records information customers type on their computers.

Here are some of the extra precautions you should take to protect yourself and your customers.

Traditional protections no longer work

Traditionally, banks have authenticated online users by requiring a login ID and password, combined with an additional layer of protection. For example, many banks use a cookie loaded onto a customer's computer to confirm that it's the same computer the customer used to enroll in online banking and that it matches the customer's login ID and password. Unfortunately, it's relatively easy for fraudsters to copy a cookie to their own computers to impersonate a customer.

For additional protection, some banks use geo-location or Internet Protocol (IP) address matching to confirm users' identities. But fraudsters have figured out how to use proxies to mimic a legitimate user's location or IP address and bypass the bank's security measures.

"Layered security" involves two or more controls for authorizing high-risk transactions.

Another common authentication technique is to use challenge questions selected by the customers during the enrollment process. Often, however, impostors are able to answer these questions. For example, a fraudster who knows the customer or is adept at online research can easily supply a customer's mother's maiden name or the year the customer graduated from college.

In light of these weaknesses, the Federal Financial Institutions Examination Council (FFIEC) in 2011 supplemented its 2005 guidance on *Authentication in an Internet Banking Environment*. The FFIEC advised banks that device authentication and basic challenge questions, used as a primary control, no longer served as effective risk mitigation techniques.

Your security may need improvement

According to the FFIEC, "Virtually every authentication technique can be compromised," so it's critical that banks avoid reliance on any single control. Instead, they should implement "layered security," which involves two or more controls for authorizing high-risk transactions. Examples include:

Sophisticated challenge questions. Challenge questions can be effective, provided they don't rely on publicly available information. It's more difficult (or impossible) for a fraudster to find out your favorite hero, for example, than it is to find out the name of your high school. It's also a good idea to use multiple challenge questions and to rotate them to avoid using all of the questions in a single session. Otherwise, it's easier for a fraudster to obtain the answers using a phishing scheme.

Another highly effective technique is to include one or more "red herring" questions. These are nonsensical questions that customers know to leave blank. For example, a customer without children might select the question "What is your daughter's nickname?" Any answer a fraudster provides will be wrong.

Out-of-band authentication. This is one of the most effective strategies for avoiding the risks associated with malware. It involves using another "channel," such as a cell phone, to verify a transaction initiated online. For example, after customers authenticate transactions on their computers, they might be required to enter a one-time-only code sent to them by text message. This makes it extremely difficult for fraudsters to take control of an account, even if they have a customer's login ID, password, and challenge question answers.

There are many other forms of layered security, including fraud monitoring and detection systems, transaction limits, antimalware software, and security tokens (such as read-only USB devices customers use to create a secure channel directly to the bank's servers). One solution is "positive pay." Under this approach, checks and ACH payments are blocked unless the payee is on a preapproved list furnished by the customer. The bank alerts the customer when unauthorized transactions are presented on the account and gives the customer an opportunity to allow the transaction.

Evaluate your risk

The right level of security for your bank depends upon its risk profile. Conduct annual online fraud risk assessments to ensure that you have sufficient controls in place. Depending on your level of risk, you also might consider engaging an IT consultant to conduct network penetration testing to reveal any security gaps.

The high cost of a data breach

How do data breaches affect financial institutions? Two recent studies attempt to quantify the potential losses. One study, by IT security firm Kaspersky Lab, estimated that the "true cost of financial data loss" ranges from $66,000 to $938,000, depending on organization size. The price tag includes legal and consulting fees, as well as lost business.

The second study, by the American Bankers Association, found that the recent Target breach resulted in an average loss of $331 per fraudulently used debit card and $530 per fraudulently used credit card.

Business plans can provide vital information on your borrowers

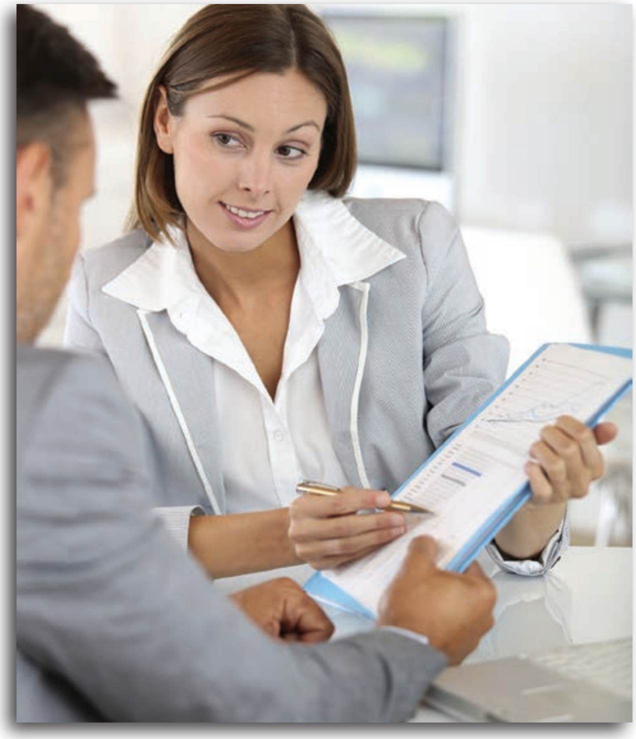
How do you know where your business customers — or potential business customers — are headed? How do you know that the strategies and actions they've planned will allow them to meet their financial goals?

Business plans provide investors and lenders with an assessment of a business's current operations, as well as its game plan for the future. They can help you gauge if your borrowers' business goals are doable.

Defining business plans

Complete plans traditionally include these six components: 1) executive summary, 2) business description, 3) industry and marketing analysis, 4) management team description, 5) implementation plan and 6) financials.

Small and midsize businesses might balk at compiling a comprehensive business plan, but it's imperative when a company is teetering on the edge of bankruptcy or needs financing for a major capital expenditure. The best plans are quite simple, however. Executive summaries can be as short as a paragraph. Long-winded plans tend to bury management's message. For small businesses, executive summaries shouldn't exceed one page, and the maximum overall length should be less than 40 pages.



Weighing in on executive summaries

Executive summaries are often the first place lenders look, but they're the last page management should write. Business planning starts with a long-term vision: Where is the company now and where does it want to be in three, five or 10 years? In other words, wise business owners start with historic financial results and then identify key benchmarks that management wants to achieve. These assumptions will drive the financials.

Sizing up financials

The second place lenders look when reviewing a business plan is the financials section. Management's goals are fleshed out in its budgets and financial projections.

For example, suppose a company with $12 million in sales in 2014 expects to double that figure over a three-year period. How will the borrower get from Point A ($12 million in 2014) to Point B ($24 million in 2017)? Many roads lead to the desired destination.

Let's say the management team decides to double sales by hiring four new salespeople and acquiring the assets of a bankrupt competitor. These assumptions will drive the projected income statement, balance sheet and cash flow statement.

When projecting the income statement, management makes assumptions about variable and fixed costs. Direct materials are generally considered variable. Salaries and rent are generally fixed. But many fixed costs can be variable over the long term. Consider rent: Once a lease expires, management can relocate to a different facility to accommodate changes in size.

Balance sheet items — receivables, inventory, payables and so on — are generally expected to grow in tandem with revenues. Management makes assumptions about its minimum cash balance, and then debt increases or decreases to keep the balance sheet balanced. In other words, your bank will be expected to fund any cash shortfalls that take place as the company grows.

The financials outline how much financing the borrower will need, how it plans to use those funds and when the borrower expects to repay its loans. As the lender, it's your job to assess whether a borrower's plan appears realistic.

Know your borrower

The rest of the business plan describes your borrower's internal and external environment. These sections demonstrate that management has done its market research and risk analysis — and truly understands the marketplace. It can be informative reading material, even if you think you know an existing borrower. ▲

When can you restore a loan to accrual status?

In the years following the recession, many community bankers faced unfamiliar accounting challenges. For example, you had to determine whether to place poor-performing loans on nonaccrual status or to classify arrangements with struggling borrowers as troubled debt restructurings.

Now, as the economy continues to improve, you face making new accounting decisions, including whether to return a nonaccrual loan to accrual status. Here's a brief review of the criteria you must consider in making this determination.

FFIEC guidance

You can find valuable guidance on restoring accrual status in the Federal Financial Institutions Examination Council's (FFIEC's) Call Report instructions. (From the home page, click on "Reports" and then "Reporting Forms." Under "Call Report Forms," click on "FFIEC 031" and then "FFIEC 031 and FFIEC 041 Instructions." "Nonaccrual Status" begins on page A-59 of the glossary.) According to the FFIEC, there are two situations in which a loan may be restored to accrual status:

1. When none of the loan's principal and interest (P&I) is due and unpaid, and the bank expects repayment of the remaining contractual P&I; *or*
2. When the loan otherwise becomes well secured (by collateral or personal guaranties) and in the process of collection (through legal action or other efforts reasonably expected to result in repayment).

Generally, to restore a loan to accrual status in situation 1, a bank must have received all past due P&I. But there are three exceptions. First, a loan may be returned to accrual status — even if the borrower hasn't yet brought all past due payments current — if:

- The borrower has resumed paying the full amount of the scheduled contractual P&I and does so for a sustained period (generally, a minimum of six months), and
- All P&I (including past due amounts) are reasonably assured of repayment within a reasonable time.

Even if a loan meets these two criteria and is restored to accrual status, the bank must continue to report it as "past due" on Schedule RC-N ("Past Due and Nonaccrual Loans, Leases, and Other Assets") of the Call Report.

The second exception is for loans that have been formally restructured in a manner that reasonably assures repayment and performance according to its modified terms. Under these circumstances, a loan need not be maintained in nonaccrual status so long as the bank supports the restructuring, and any charge-off taken, with a current, well-documented credit evaluation of the borrower's financial condition and its prospects for repayment under the revised loan terms.

The third exception is for loans acquired at a discount from an unaffiliated third party (such as another bank or a receiver of a failed bank). A bank need not maintain nonaccrual status for these loans, even though they haven't been brought current, so long as they meet the criteria for amortization outlined in AICPA Practice Bulletin No. 6 ("Amortization of Discounts on Certain Acquired Loans").

Recognition of interest income

Once a loan is placed back on accrual status, questions arise regarding the treatment of interest payments made while the loan was in nonaccrual status. When a loan is in nonaccrual status, the bank stops accruing interest income. In some cases, banks recognize interest payments actually received on a cash basis, but typically they apply these payments to principal.

When a loan is restored to accrual status, should the bank reverse the application of these payments to principal and instead apply them to interest income? The FFIEC says "no." Instead, after a loan is placed back on accrual status, the bank should begin recognizing interest income *prospectively*, based on the loan's recalculated effective yield to maturity.

A case-by-case decision

Each loan and borrower is different, and predicting the likelihood that a loan will be repaid requires significant judgment on the part of bank management. To determine whether a loan should be returned to accrual status, evaluate it based on its particular facts and circumstances, with the help of your financial advisors if necessary.

The Office of the Comptroller of the Currency produces a *Bank Accounting Advisory Series* that includes several factual situations and the suggested handling of nonaccrual loans. The most recent version was published in September 2013. (At occ.gov, click on "Publications." Under "Publications by Type," click on "Other Publications/Reports." The link to the *Series* is under "Legal and Accounting Publications.") ▲

B A N K

Wire

FDIC GIVES INSIGHT INTO EXAM TRENDS

Loans and board and management issues were the two most-cited categories deemed to be “matters requiring board attention” (MRBAs) in an article in the FDIC’s *Supervisory Insights*. The article sums up significant trends based on categories cited most often by examiners at satisfactorily rated institutions.

Within the loan category, 75% of MRBAs were related to credit administration, including the need to:

- Improve appraisal review, loan review, and the loan grading system,
- Reduce credit data or collateral documentation exceptions,
- Prepare cash flow analyses, and
- Properly account for troubled debt restructurings.

About 41% of loan-related MRBAs addressed elevated levels of problem assets, while about 28% involved deficiencies in the allowance for loan and lease losses.

The most common board and management issues concerned audit deficiencies; needed improvements in strategic planning, succession planning, and risk management practices; and the revision of, and compliance with, board-approved policies.

Other commonly cited categories included violations, earnings, interest rate risk, IT and liquidity. ▲

MORTGAGE SERVICING VIOLATIONS AND DECEPTIVE FREE CHECKING ADS CITED

In September, the Consumer Financial Protection Bureau (CFPB) took action against a Michigan bank for violating the new mortgage servicing rules. Violations included: 1) taking “excessive time” to process borrowers’ applications for foreclosure relief, 2) failing to alert borrowers about incomplete applications, 3) miscalculating incomes, and 4) denying loan modifications to qualified borrowers.

The CFPB ordered the bank to pay $27.5 million to those borrowers, plus a $10 million penalty.

In October, the CFPB took action against a New York bank for deceptively advertising free checking accounts. The bank promised free checking with “no strings attached,” but failed to disclose that customers who didn’t meet certain eligibility requirements — including a minimum level of account activity — would automatically be switched to fee-based accounts.

The CFPB ordered the bank to pay a $200,000 penalty and to refund $2.9 million in customer fees. ▲

ARE BANKS USING THE CLOUD?

In a recent survey, *American Banker* asked, “How much does your bank use cloud computing?” A slim majority said “not at all.” Here are the responses:

- Not at all — The security risks are too high (52%).
- A little — Only for non-mission-critical apps, such as risk modeling (26%).
- A lot — The lower cost and flexibility make hosted software a no-brainer (22%).

Although many banks continue to have security concerns about cloud computing, it doesn’t mean you shouldn’t use it. But if you’re considering a move to the cloud, learn the risks involved and how to manage them. ▲

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