

Community Banking

A D V I S O R

Winter 2012

Clocking customers' growth

Watch out for expansion
that can veer out of control

**IT security: Is your
program still effective?**

BANK Wire

Take a balanced approach to incentive compensation



**MAULDIN
& JENKINS**

800-277-0080 | www.mjcpa.com

Take a balanced approach to incentive compensation

For many banks, a strategically designed compensation plan — one that includes performance incentives — is critical to success. Incentive compensation can help a bank attract and retain high-quality executives and other employees and motivate them to enhance the institution's performance.

Conversely, a poorly designed program can encourage executives to engage in activities that maximize short-term returns while putting the bank's long-term health at risk.

Misaligned incentives

Incentive compensation can take a variety of forms, including cash bonuses and equity-based incentives such

as stock options, restricted stock and stock appreciation rights. Regardless of which tools banks use, the objective is generally the same: to align employees' performance goals with the bank's goals.

Many banks' incentive plans tie compensation to increased short-term revenue or profits, which can encourage employees to engage in excessively risky activities.

One reason that equity-based incentives are so popular is that they align employees' interests with those of the shareholders. In other words, giving employees an ownership interest in the bank motivates them to maximize shareholder value. Unfortunately, many banks' incentive plans tie compensation to increased short-term revenue or profits, which can encourage employees to engage in excessively risky activities.

Let's say that Good Samaritan Bank pays loan officers bonuses if they meet or exceed a specified level of loan originations. This approach provides no incentive to seek loans that meet minimum asset quality standards. In fact, it has the opposite effect — loan officers earn more if they *lower* their standards. This may boost their short-term rewards (as well as short-term returns for shareholders), but it endangers the bank's long-term stability.

Risk vs. reward

In 2010, the FFIEC issued its *Interagency Guidance on Sound Incentive Compensation Policies*. According to the guidance, "Flawed incentive compensation



practices in the financial industry were one of many factors contributing to the financial crisis that began in 2007.” The agencies felt that, too often, banks offered incentives to employees who increased short-term performance, “without adequate recognition of the risks” to the bank.

The agencies also observed that, in banking, it may not be enough for an incentive compensation plan to align the interests of employees and shareholders. That’s because the “federal safety net,” which includes federal deposit insurance and access to the Federal Reserve’s discount window and payment services, often leads bank shareholders to tolerate risk levels that are inconsistent with safety and soundness principles.

3 key principles

To help banks design incentive compensation programs that are both safe and effective, the guidance focuses on three key principles. Incentives should:

1. Appropriately balance risk and reward,
2. Be compatible with effective controls and risk management, and
3. Be supported by strong corporate governance.

The guidance also identifies four methods currently used — either alone or in combination — to build risk into the compensation decision: risk-adjusted awards, deferred payments, longer performance periods and reduced sensitivity to short-term performance.

Good Samaritan Bank, for instance, might adjust incentive compensation for risk by including performance targets not only for the dollar amount of originations,

New compensation rules could “trickle down” to community banks

The federal banking agencies’ April 2011 proposed rule on “Incentive-Based Compensation Arrangements” essentially would codify much of the interagency guidance discussed in the main article, imposing specific requirements on large financial institutions. As of this writing, the agencies are still reviewing comments on the proposal and plan to issue a joint final rule.

For institutions with at least \$1 billion in consolidated assets, the rules would prohibit incentive compensation arrangements that encourage inappropriate risk by providing executives or other key employees with “excessive compensation” or compensation that could lead to a “material financial loss.” And institutions with at least \$50 billion in total consolidated assets would be required to defer at least 50% of incentive compensation for certain key executives for at least three years.

The proposed rules wouldn’t apply to community banks. But once finalized, they may establish best practices for incentive compensation that will have a “trickle down” effect on smaller institutions.

but also for asset quality or compliance with documentation or other administrative standards. Additionally, the bank might defer a portion of a loan officer’s bonus for a few years and adjust it downward, if necessary, to reflect nonperforming loans. Similarly, compensation tied to profits might be based on longer performance periods to provide employees with an incentive to focus on the bank’s long-term performance.

The agencies advise banks to integrate incentive compensation into their risk-management and internal control frameworks and to monitor and measure their incentive programs for balance, effectiveness and actual risk outcomes. Banks also should ensure that their incentive compensation programs are supported by strong corporate governance, including active and effective oversight by their boards of directors.

Review your program

Although the guidance imposes no specific *requirements*, it’s a good idea to review your compensation program with the agencies’ recommendations in mind. Expect regulators to scrutinize your incentive arrangements to ensure that they are aligned with the institution’s long-term financial health and don’t promote inappropriate risk-taking. ▲

Clocking customers' growth

Watch out for expansion that can veer out of control

When a loan customer's business is booming, it's easy to be enamored by the outward signs of prosperity. But, if you don't watch out for risky behavior, your borrower could be heading for trouble. Consider this hypothetical case.

What can happen

A food safety firm grew at an average annual rate of 220% in its first 10 years. Its owners were so focused on gaining new business and developing products that many administrative tasks — licensing, quality control, training, collections and others — fell by the wayside.

Then the company maxed out its credit line. Fortunately, its lender dropped by to discuss the business's voracious appetite for financing. The lender also needed to address customer complaints about sloppy equipment installation and supplier protests about delinquent payments.

How control can be restored

If caught before a borrower careens out of control, rapid growth can be decelerated to a more sustainable rate. On the advice of their lender, the food safety firm



owners regained control by categorizing their customers by size and profitability. Next they eliminated small, low-margin jobs that weren't worth the effort. Then they hired an operations manager to oversee quality control, regulatory compliance and training.

Additionally, the owners started requiring salespeople to check credit on all new accounts, and they based sales commissions on collections, not gross sales. They also diversified their customer base, so no individual account represented more than 15% of annual sales. Plus, the owners implemented price increases, which eventually reduced demand but helped increase profit margins.

What to watch for

One of the biggest challenges high-growth firms face is finding enough financing for all their expansion plans. They think, "If you want to double sales, double assets."

Buying machines, computers and other assets requires debt or equity financing, which can be good for the lender in the short term but possibly perilous for the borrower. Overzealous asset acquisition strategies can cause repayment problems if cash flow projections fall short.

There's also delay between when a growing business buys inventory, makes products and pays employees (cash outflows) and when it receives payment from customers (cash inflows). The faster the growth, the bigger the gap. Businesses typically fund the shortfall with a credit line. And as the firms take on more and more debt, loan repayments eventually consume all (or most) of cash flows.

Moral to the story

There's a moral to the fast-growth story: When a lender keeps an eye on the borrower's debt-equity ratio and profit margins, it can put the brakes on lending if the time is right. Sometimes less — or slower — is more. ▲

IT security: Is your program still effective?

As online banking services become more sophisticated and more widely used, IT security measures that were effective only a few years ago may no longer be enough.

In June 2011, the FFIEC issued *Supplement to Authentication in an Internet Banking Environment*, urging banks to tighten their controls on customer authentication. The FFIEC chose to revisit guidance originally issued in 2005 because common authentication methods and controls have “become less effective” in an “increasingly hostile online environment.”

In light of the updated guidance, your bank should conduct an IT risk assessment and, if needed, implement more-complex customer authentication procedures as well as extra layers of protection.

Hackers increasingly sophisticated

Many banks responded to the 2005 guidance by implementing simple authentication procedures. But the FFIEC now recognizes that these techniques are insufficient to thwart today's hackers.

The supplementary guidance recommends “layered security,” which means different controls at different points in the transaction process.

For example, a bank might load a “cookie” onto a customer's computer to confirm that the username and password match the computer originally used to enroll the customer. But today hackers can easily



copy these cookies to their own computers and then use them to impersonate the customer.

A more effective approach is to use more complex device identification techniques, which use “one-time” cookies to confirm not only the computer's configuration, but also its IP address, location and other characteristics.

Simple “challenge” questions also are vulnerable, because hackers can easily learn the answers — such as the customer's mother's maiden name or the street where the customer grew up — with a little research. A better approach is to 1) design challenge questions based on nonpublic information, 2) include “red herring” questions that will trip up hackers but that customers will recognize as nonsensical, and 3) set up multiple challenge questions and use different sets of questions in each online banking session.

Layered security offers more protection

It's no longer sufficient to rely on one form of customer authentication, according to the FFIEC. The supplementary guidance recommends “layered security,” which means different controls at different points in



the transaction process. This allows the strength of one control to compensate for weaknesses in other controls.

The number of layers depends on the level of risk. According to the FFIEC, for example, commercial customers generally present more risk than retail customers. That's because commercial customers tend to conduct more frequent transactions in higher dollar amounts and make more use of ACH file origination and interbank wire transfers.

One of the most effective layering strategies is “out-of-band” authentication of high-risk transactions. In other words, a transaction initiated through one channel — the Internet, for instance — must be verified or reauthenticated through another channel, such as the telephone. Once a transaction has been authenticated by a customer via computer, for example, some banks require the customer to input a code sent by text message to the customer's cell phone.

These measures are important because even multiple authentications via the same device are vulnerable to attack. Consider keylogging malware. These software programs, which can be installed by visiting an infected website or downloading an e-mail attachment, record a customer's computer keystrokes and transmit them over the Internet to a hacker.

Because the malware can be used to steal a customer's logon ID and password, as well as the answers to challenge questions, it can overcome dual authentication strategies. Out-of-band authentication makes this far more difficult.

Antimalware software can provide an additional layer of protection. Like antivirus software, these programs help prevent, detect and remove malware before a hacker has a chance to use it.

Regulators call for other controls

The new guidance also recommends these tools and tactics:

- Fraud monitoring and detection systems, which alert the bank to anomalies based on a customer's history and behavior patterns,
- Positive pay, which limits check payment to those on a preapproved list supplied by the customer,
- Transaction limits (on transaction value, payment recipients or number of transactions per day),
- Payment windows, which restrict payments to certain days and times, and
- Read-only USB devices that customers plug into their computers to create a secure channel directly to the bank's servers and that aren't susceptible to malware.

It's also important to show customers how to protect themselves. Banks should educate customers on, for example, how to select an effective password, whom to contact in case of suspicious activity, and the circumstances under which the bank might request the customer's authentication information.

Get with the program

To ensure that your bank's IT security program continues to be effective in the current environment, conduct periodic risk assessments and enhance your controls and customer education efforts as needed. Implementing the FFIEC's supplementary guidance also will help you convince bank examiners that your IT security efforts are adequate. ▲



FAF: NO INDEPENDENT BOARD FOR "PRIVATE COMPANY GAAP"

The Financial Accounting Foundation (FAF) has rejected the concept of a separate accounting standards board for private companies, despite a recommendation that it establish such a board from the Blue-Ribbon Panel on Standard Setting for Private Companies.

The Blue-Ribbon Panel — sponsored by the FAF, the AICPA and the National Association of State Boards of Accountancy — concluded that an autonomous board would “better respond to the needs of the private company sector.” The panel envisioned a board that would develop appropriate private-company exceptions and modifications to U.S. Generally Accepted

Accounting Principles (GAAP) and work closely with FASB to incorporate these changes into the Accounting Standards Codification (ASC).

The FAF proposed instead to establish a Private Company Standards Improvement Council (PCSIC). The PCSIC would identify appropriate exceptions and modifications to GAAP for private companies, subject to ratification by FASB. The FAF’s trustees felt that establishing a separate board for private companies would lead to two separate sets of accounting standards — a “big GAAP” for public companies and a “little GAAP” for private companies. ▲

A HANDY GUIDE TO THE FAIR CREDIT REPORTING ACT

Until recently, the Federal Trade Commission (FTC) was responsible for interpreting and enforcing the Fair Credit Reporting Act (FCRA). While the FTC continues its enforcement role, the newly established Consumer Financial Protection Bureau (CFPB) now has primary responsibility for interpreting the FCRA and issuing regulations.

In part to smooth the transition to the CFPB, in July the FTC published *40 Years of Experience with the Fair Credit Reporting Act: An FTC Staff Report with Summary of Interpretations*. You can download this helpful guide at ftc.gov. (Click on “Actions / Documents / Commission & Staff Reports / 2011.”) ▲

ARE YOU COMPLYING WITH SCRA?

A recent hearing before the House Committee on Veterans’ Affairs revealed widespread mortgage-related violations of the Servicemembers Civil Relief Act (SCRA).

The SCRA provides financial protection for members of the armed services during periods of active duty. Among other things, the act requires banks to reduce interest rates on certain mortgage and nonmortgage loans and refrain from foreclosing without a court order.



Further, the Veterans’ Benefits Act of 2010 gives service members a private cause of action for SCRA violations, allowing them to sue banks for damages, injunctive relief and attorneys’ fees.

This development, combined with the struggling real estate market and worldwide military activity, has increased the frequency of SCRA litigation against banks. So check that you have systems in place for ensuring SCRA compliance and monitoring changes in the act’s requirements. ▲



200 GALLERIA PARKWAY, SE | SUITE 1700
ATLANTA, GA 30339
800-277-0080 | www.mjcpa.com

Other offices:

Albany, GA | Macon, GA | Birmingham, AL | Bradenton, FL



Financial Institution Services

At Mauldin & Jenkins, we have more than 90 years of experience providing audit, tax and advisory services to financial institutions. We understand audit requirements, tax planning strategies, compliance and more. With a dedicated team focused on providing services to financial institutions, we are a recognized and proven leader. Our services include:

- External & Internal Audits
- SOX 404 / FDICIA Internal Control
- Tax Planning & Preparation
- Employee Benefit Plan Audits
- Mergers & Acquisitions
- Compliance & Bank Secrecy Act Reviews
- Loan Reviews
- Risk Management

A history of success built one satisfied client at a time!