

SERVICING MANAGEMENT®

Reprinted with permission from the October 2006 issue

The Risks And Rewards Of Privacy-Compliant Product Marketing

Privacy compliance and marketing initiatives might seem incompatible, but both can be successfully achieved on the same path.

BY GREG GENUA

Privacy-compliant optional product marketing can help solve problems such as decreasing net profit margins, increased risk and high costs to service. It can also help servicers fund important strategic initiatives and prepare for the next refinancing wave.

The current restrictive regulatory environment can seem overwhelming. But what few servicers know is that optional product marketing (OPM) can generate per-loan revenues of \$2, \$6 or even \$14 and higher to fund their critical objectives without significantly increasing their risk.

The highly profitable annual revenues from OPM can easily reach six figures for smaller servicers and exceed seven figures for mid- and large-sized shops. Servicers can no longer afford to give minimal attention to OPM or ignore its impact on their balance sheets.

While the privacy vs. marketing issue has a long history and can present a fair amount of conflict, it is not insurmountable. One essential requirement is that the servicing industry self-evaluates and thoroughly understands both sides of the equation.

Greg Genua is a certified information privacy professional with over a decade of experience in the mortgage banking industry. He is an independent consultant and can be reached at greg@genua.us or (918) 451-2247.

Results from recent surveys of executives and managers regarding privacy-security issues are alarming and reflect deep concerns that need to be addressed. Key findings and conclusions show a high awareness of risks and associated costs. However, corporate executives and industry leaders express minimal confidence that widespread organizational compliance is adequate.

Privacy background

The mortgage industry's experience with privacy began in the 1970s. It evolved with more onerous privacy-related regulations, such as the Gramm-Leach-Bliley Act (GLBA), the USA Patriot Act and the Fair and Accurate Credit Transactions Act. As if that were not enough, as of March 2006, there were 22 proposed federal bills and 642 proposed state bills related to privacy and data security.

It has been six years since GLBA was enacted. It appears that our industry still doesn't appreciate, or has underestimated, the full scope and impact that privacy has on their operations and total risk exposure. Given the heightened public awareness and investor sensitivity, the consequences of any privacy-security breach are immediate and quantifiable. There is an average 2% to 4% corresponding stock decline immedi-

ately following a company's announcement of such a breach. Non-compliance has ramifications that include financial risk (corporate and personal) and, in extreme cases, incarceration.

Equally important, servicers have yet to capitalize on OPM to the fullest extent possible and gain the reward of exponential revenue growth. Despite the obvious, it does not appear that either privacy or OPM has been assigned the appropriate priority. This is evidenced by a general deficiency among companies to establish executive-level positions for privacy or marketing.

If corporations operated without a chief executive officer or chief financial officer, those companies would be viewed as suspect by investors and Wall Street, and their own boards of directors would force change. The same opinion is developing about companies that lack executive leadership for corporate-wide privacy and marketing initiatives. These new positions should fully monitor and manage privacy and marketing, as well as be accountable for the profit and loss profiles of these separate entities, business units or departments.

Organizations that operate globally or outsource offshore must contend with the contrasting privacy laws in Europe, Canada and the Asia Pacific



region (Japan, Hong Kong, Singapore, Australia, etc.) At this time, India is considered an emerging privacy environment, and several new laws are being developed there. Privacy-marketing best practices should be created and documented. Companies then must adhere to and execute procedures that range from mailroom functions to Web site attestation.

New developments

Companies face new and compelling developments regarding privacy issues. There is an escalating battle between federal and state bodies for preemption. Financial institutions must demonstrate compliance competency throughout their operational functions. Federal agencies are wrestling with standardizing language to make privacy policy notices more consumer-friendly.

The federal vs. state territorialism is more than a squabble. It is both serious and complicated. We have known for some time that the flood of state legislation could test the federal preemption position. The pressure has been building, and that levee has developed its first crack. The U.S. Supreme Court has agreed to review *Wachovia v. Watters* - a prominent preemption case - and the outcome could release a torrent of similar actions and produce a wave of new obligations.

Major operational process flaws can hide in the simplest functions. Delivering privacy notices and executing opt-out requests, computer network security and laptop protection are but a few. Third-party issues, including data-sharing, outsourcing direct mail or telemarketing, can further complicate the situation. If any of these functions are managed poorly, it could trigger negative actions against your company.

The standardization of privacy notices or any requirement for a major rewrite would drain the resources of all financial institutions. Servicers would have to go back to what they say (language) and how they communicate it (print, verbal, Web site, etc.) and reevaluate every process and

procedure that supports privacy compliance.

This year, the Federal Communications Commission proposed fines against two well-known telecom providers - not for actually exposing or releasing customers' records, but simply because they failed to provide accurate certification that they have protected their customers' data. This trend is affecting other industries, and it will likely spill over into mortgage servicing and force companies to scramble to comply.

Reducing the cost to service is an ongoing objective with serious consequences. Servicers are pressured to evaluate and control every operational expense, including salaries, temporary personnel use, cost per call, average talk time, automation and offshoring. Despite the optimistic initial projections regarding cost savings through offshore outsourcing, many of those engaged are struggling to hit targets or have not fully realized their expectations.

Funding will be needed for special projects or initiatives that are vital to a corporation's vision and strategic plan for long-term growth. The problem is that most business units or departments have already been scrutinized and trimmed to operate as efficiently as possible.

Compliance and profitability

The requirements of recent privacy regulations have elevated risk exposure, increased costs, expanded the scope of executive accountability and obligated detailed documentation from operational management and frontline personnel.

Today, federal regulatory agencies hold executives responsible for everything from privacy compliance to accounting activities. Of course, executives are expected to concurrently generate the highest possible profitability or shareholder value.

In support, servicing managers must maximize operational efficiency, ensure that customers' rights are being respected and produce detailed documentation for the most basic servicing functions. Additionally,

managers are asked to continually improve the return on expenses while reducing the cost to service - all while industry trends show evidence of constricting margins. Some organizations have even applied the blanket policy of haphazard cost-cutting.

Despite all these issues, it is still possible for mortgage servicers to balance privacy compliance with OPM to experience 50%, 100% or even 200% growth on their revenues per loan. These growth projections exclude phone pay or alternative collection fees, lender-placed hazard insurance or any associated late fees.

OPM may not be the core business, but it can generate annual revenues ranging from \$2 to \$6 per loan for servicers that perform OPM sparsely. For servicers that are conducting regular OPM strategies, revenues can be increased to \$8 to \$14+ per loan. Initial increases in cash flow can occur within six to 12 months. When developed correctly, OPM revenues will offset the minor expenses associated with additional infrastructure, resource support, staffing or consulting fees.

Considering this revenue potential, it should not matter whether net gains are added to the corporate income statement as net pre-tax income, earmarked for special projects or used as a direct offset to the cost to service. Whatever the accounting treatment is, it can make a noticeable difference.

A word of caution about realizing insurance revenues is warranted. Some servicers are taking OPM insurance revenues without having the appropriate insurance licenses. In most cases, a federal status (charter or regulatory reporting treatment) will not preclude companies from having to deal with states' attorneys general, banking regulators or departments of insurance.

Some servicers take insurance revenues in the form of flat fees on a per-policy or account basis. This approach exposes both the financial institution and insurance product provider to risks, provides only marginal protection and leads companies down a very slippery slope. Costs associated with getting licensed are

minimal when compared to multi-million dollar litigation or, conversely, millions of dollars in potential revenues.

Taking action

The initial, critical steps to understanding and implementing OPM solutions include securing a project champion at the executive level, performing gap analysis on current privacy compliance and OPM, reviewing lender-placed insurance activities, documenting the various customer communication channels, evaluating personnel skill sets for task assignments and building consensus.

Other important steps include es-

tablishing a reporting structure, appointing or hiring an executive-level leader, developing OPM benchmarking and annual budget planning, determining where the revenue will be applied, promoting awareness and accountability within the customer service unit, and creating monitoring tools and procedures regarding customer noise specific to OPM. Additional work includes process mapping, vendor contract review, systems evaluation and timeline development.

The servicing industry appears to still have many gaps between the perception of privacy compliance and the reality of operational execution. The continuing dilemma is to find

compatibility that facilitates OPM without adding undue risk.

The bad news is that risks are here to stay, and they will only increase. The good news is that OPM is a way to fund privacy compliance and garner enough excess revenue to solve many business needs.

For most servicers, the potential revenues from OPM remain virtually untapped. OPM is a capital resource that is meaningful and deserves consideration. In the past, privacy compliance and OPM seemed incompatible and unimportant. Today, they are inseparable and relevant. Tomorrow, they will be instrumental and a key driver for success. **SM**