The very dangerous intersection of UDAAP and vendor mismanagement

By Martin J. Bishop

(Martin J. Bishop is vice chair of the Litigation Department and co-chair of the Consumer Financial Services Practice atFoley & Lardner LLP. He can be reached at mbishop@foley.com.)

Thomson Reuters News & Insight
September 28, 2012

The competition for consumers in the financial services industry can be fierce. Financial institutions need to stay competitive by offering cutting-edge products and expanding and improving services. More and more frequently, financial institutions are looking to third-party vendors to help them cut costs and deliver products and services to consumers that the financial institutions simply do not offer. But this is far from a risk-free proposition.

Historically, regulators like the Office of the Comptroller of the Currency ("OCC"), the Federal Reserve Board ("Federal Reserve"), and the Federal Deposit Insurance Corporation ("FDIC") have, in one way or another, required financial institutions to oversee their vendor relationships and manage the corresponding risks. The Consumer Financial Protection Bureau ("Bureau") has recently weighed in on vendor management in a big way.

THE CAPITAL ONE ENFORCEMENT ACTION AND CONSENT ORDER

In July of this year, the Bureau announced the conclusion of its first public enforcement action, the result of which is that Capital One Bank, N.A. ("Capital One") must return approximately $140 million to an estimated two million consumers and pay a $25 million dollar civil penalty to the Bureau's Civil Penalty Fund. These refunds and penalties are on top of million of dollars of refunds and a $35 million penalty assessed by the OCC. What led to these significant refunds and steep penalties? Vendors.

The Bureau – which was acting pursuant to its power to prevent unfair, deceptive, or abusive acts or practices ("UDAAP") under the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act") – found that Capital One's call center vendors were deceptive when selling Capital One's credit card add-on products. According to the Bureau, the call center vendors used high-pressure sales tactics to sell these products to consumers with low credit scores or low credit limits when the consumers called to activate their cards.

Specifically, the Bureau claims to have discovered during its supervision of Capital One that consumers were, among other things, misled to believe that certain add-on products would improve credit scores or credit limits. The call center apparently did not always tell consumers that the add-on products were optional or that there was a cost associated with the product. In some cases, the call center vendors enrolled consumers in add-on products without the consumer's consent. There is more, but you get the gist: the Bureau does not want to see vendors pressuring and deceiving consumers about the nature of the transactions they are entering into.

OTHER UDAAP PRONOUNCEMENTS BY THE BUREAU

The consumer financial services industry has waited and waited for the Bureau to make a significant statement about how it intends to use its vague and seemingly boundless UDAAP powers. What is most unfortunate is that further pronouncements about UDAAP are likely to come by way of enforcement actions rather than rulemaking.

Of course, we have heard Bureau Director Richard Cordray say things publicly about UDAAP. Earlier this year, Director Cordray noted that the Bureau has "given some exam guidance around these concepts, and I think maybe we'll have more to say over time." With the Capital One enforcement action, that statement sounds hauntingly prophetic. And while it is true that the Bureau has made some modest

statements about UDAAP in its Supervision and Examination Manual, a lot of what the Bureau has said overall has been too abstract to be meaningful, particularly in the context of a new regulator with expansive powers to apply novel standards under the sometimes less-than-obvious provisions of the Dodd-Frank Act.

WHAT CAN BE DONE UNDER VAGUE DEFINITIONS AND UNHELPFUL GUIDANCE?

With the Capital One settlement, the Bureau has clearly identified the intersection between vendor management and UDAAP. In its press release announcing the Capital One settlement, the Bureau stated that it is putting "other institutions on notice that [the Bureau] will not tolerate deceptive marketing practices, and institutions will be held responsible for the actions of their third-party vendors." In an accompanying Bureau bulletin, the Bureau outlined its "expectation" that every institution under its supervision "and their service providers" will comply with Federal consumer financial law, which includes the Dodd-Frank Act's UDAAP prohibition.

And the Bureau is not content to just warn the industry that it is serious about enforcing UDAAP and punishing financial institutions for UDAAP violations committed by their vendors. The Bureau is being proactive, and not just by fully utilizing its supervision powers. On the heels of the Capital One settlement, the Bureau began actively and publicly recruiting investigators to work undercover and pursue cases against financial institutions. These "secret shoppers" will receive between $98,000 and $150,000 and, presumably, will be – may already be – out there looking for UDAAP violations wherever they can find them.

So here you are – smack dab in the middle of the intersection of vendor management and UDAAP. What can you do to mitigate your risks? What can you do to avoid the potential of hundreds of millions of dollars in restitution and penalties like we saw with the Capital One settlement? Two critically important things: (1) manage your UDAAP risks, and (2) manage your third-party vendor risks.

MANAGING UDAAP RISKS

Until there is more guidance from the Bureau on UDAAP, it is important to keep some of the most basic principles of risk management at the fore. What follows here are ten or so suggestions that can help manage and even minimize the risk of UDAAP problems with vendors.

First, whenever possible, get lawyers and compliance officers conversant in UDAAP into the room where vendor management and oversight programs and processes are being developed and discussed. This is not to have someone in the room to say "no" early and often. Rather, among other things, this can help risk managers better understand the development process and help business lines make adjustments long before they reach the point of no return.

Second, vendors should be incentivized to be compliant and otherwise engage in ethical conduct. While even "trying" in the UDAAP environment may be difficult and not enough to completely avoid the Bureau, it should go a long way to mitigate the intensity of the heat that follows along with a UDAAP investigation.

Third, if your vendors are interacting with consumers, make sure they facilitate informed choices by customers. Vendors should be focusing consumer attention on things like limitations, conditions, and other key terms in financing documents.

Fourth, and somewhat related, make sure that you and your vendors are thinking about suitability in an expansive way. As suitability continues to develop as an ever-intensifying and elastic concept, everyone needs to stay focused on whether consumer financial products and services are suitable for the targets, and even suitable for specific consumers.

Fifth, be proactive with your vendors, and encourage your vendors to be proactive. Financial services companies, banks, and their vendors should all seek input about products and service from customers

and employees alike. The Bureau is doing this very effectively, and you should too. Make it safe for employees to raise questions or concerns about company products and services.

Sixth, focus on consumer complaints about the vendor. It may make sense to consolidate product and service complaints so that discernable complaint trends do not get ignored by your institution or your vendors. Where there is controversy, scrutinize it to determine if there may be lurking UDAAP issues.

Seventh, consider conducting a comprehensive UDAAP audit of not only your own products and services, but those of your vendors as well. An audit is a matter of due diligence, the lack of which has the very real potential to be catastrophic. Be sure to couple UDAAP audits with comprehensive training and to reinforce training with regular training updates.

Eighth, monitor what your vendors are doing by including periodic reviews of the internet and social media sources. The Bureau is all over this, and you should be, too. There is a virtual cyclone of information out there and if you don't stay on top of it, you run the very real risk of getting whisked away by it.

Ninth, when you partner with a vendor, demand that they have "skin in the game." There is no better regulator than a fiscal one. Where vendors have incentives tied to their compliance and performance, they will work that much harder at complying with UDAAP.

Tenth, and finally, if you have laid out a public statement about your institution's intention to comply with UDAAP (if you have not, you should at least consider it), ask your vendor to do the same. The statement can be anywhere (and everywhere if you choose) – loan documents, credit card statements, websites, marketing materials – anywhere prominent. This forces your vendors to think about UDAAP, as they are essentially telling the public – including your customers and your regulator(s) – that they intend to comply with UDAAP.

MANAGING THIRD-PARTY VENDOR RISKS

The Federal Financial Institutions Examination Council ("FFEIC") has done everyone a bit of a favor by compiling the guidelines regarding, among other things, the management and oversight of vendors. As a general matter, regulators assume and expect that many (most?) vendor relationships should be exposed to the same consumer protection policies that regulators expect from consumer financial services companies. With this expectation and the UDAAP management principles discussed above in mind, what can you do to provide your senior management and board of directors with the information they need to oversee the risks associated with vendor management?

The FFEIC Handbook or "Interagency Guidelines," which includes the guidelines of the various regulators (i.e., the OCC, the Federal Reserve, and the FDIC), lays out four important rungs on the ladder that is the life cycle of vendor relationships, beginning with the pre-contracting phase and carrying straight through to the implementation and maintenance of the relationship. The rungs, each discussed below, are: (1) assessing the risk; (2) conducting due diligence; (3) negotiating and structuring contracts; and (4) continuing monitoring of vendors.

Assessing the Risk

Financial institutions and consumer financial services companies assess risk, as a general matter, by identifying compliance dangers and weaknesses, and then determining the impact those dangers and weaknesses could have on an institution. The risks and dangers are virtually unlimited, but include threats to operations, strategy, reputation, specific transactions, and legal and compliance threats. The Interagency Guidelines suggest that management consider several factors in appraising these and other risks.

Specifically, for risks that relate to a vendor's function for the institution, management and the board should consider things like the sensitivity of the data being accessed or controlled by the vendor.

Similarly, management should consider the volume of transactions being performed by the vendor and how critical the vendor's function is to the business of the institution. If the vendor is interacting with consumers, designing products, or developing terms, you will need to determine whether the vendor relationship will give rise to new UDAAP risks.

Risks related to a vendor's function are not, of course, the only risk. Institutions must also review the risks concerning the vendor itself. Have you reviewed the vendor's management? Has there been turnover? Has there been significant turnover with the vendor's employees? How strong are the vendor's finances? Is the vendor well positioned to maintain a sustained and long-lasting financial relationship? Is it susceptible to business interruptions? Does the vendor have experience in consumer relations and mitigating UDAAP risks? In addition to getting answers to these questions, management will need to determine whether the vendor can provide accurate and timely information when needed, has experience with the outsourced function, and is itself reliant on other vendors.

Another important risk to assess is technology. Is the vendor using reliable technology? Is it secure? Can it accommodate growth (i.e., is it scalable?)? Risk here can also give rise to UDAAP risk.

While it may seem obvious to some, in today's regulatory environment, consumer financial services companies must avoid taking on more risk than it can effectively manage, monitor, and control. This is the heart of the risk assessment review.

Conducting Due Diligence

Due diligence follows closely on the heels of risk assessment and, in some ways, overlaps portions of the risk assessment review. Due diligence, however, is less subjective and more qualitative and quantitative. The scope of a due diligence review is typically related to the importance of an institution's relationship with its vendor; the more important a vendor's role to an institution, the more extensive a due diligence review may (and likely should) be.

What are the typical considerations when conducting due diligence on a vendor? A vendor's financial condition is one very important consideration. A due diligence review of a vendor with a low level of importance may be complete by a review of recent balance sheets and income statements. More important vendors may require due diligence at a much deeper level and would include reviewing company audits, SAS-70 audit reports, SEC filings, or even conducting an independent audit. One other important consideration in examining a vendor's financial condition is preparedness for disaster or catastrophe; i.e., what kind of insurance does the vendor maintain for contingencies like fire, data or document loss, liability, and fidelity bond coverage? Engaging fiscally weak vendors that engage in conduct that harms consumers as a result of that fiscal weakness could give rise to unfairness arguments under UDAAP.

Any due diligence review should include a review of the vendor's operations and staffing. How does the vendor handle consumer's confidential information? What are the vendor's policy and protections with respect to record maintenance? Does the vendor do employee background checks during the application process? Does it follow-up with periodic checks during employment? What is the vendor's employee turnover rate? Is management consistent and stable? Does the vendor conduct UDAAP training? How does it monitor its employees interactions with consumers?

In addition to these important considerations, the due diligence process should also reveal the vendor's reputation (e.g., through references from other financial services companies and searches through publicly available sources such as the internet), problem solving-skills (e.g., how will the vendor handle a service disruption?), and whether the vendor's physical location(s) heightens risk (e.g., is the vendor located offshore?).

Once the due diligence process is complete, it is important to capture and memorialize the critical findings. You should then spell out the vendor's responsibilities for notification of deviations from those findings and your institution's recourse if there are significant resulting issues.

Negotiating and Structuring Contracts

Contracts are, as we all know, the memorialization of the terms of the parties' agreement, and they can be written or oral. For vendors, it is important to reduce any and all terms to writing. Contract negotiations often yield clear understandings between the individuals negotiating the contract as to certain aspects of the arrangement. Sometimes those aspects are less clear to bystanders to the negotiations. If the parties fail to memorialize these understandings in a coherent way, one or both parties may lose the benefit of their bargain at some point in the future. Thus, it is wise to keep comprehensive notes during the negotiation process and bring counsel in whenever appropriate to ensure that everything you understand the vendor has agreed to finds its way into the final document that the parties will sign.

While every deal is likely to be different, there are some common terms that you should always include in your vendor contracts. First, spell out the scope of the parties' relationship. Second, include the vendor's responsibilities and how you intend to measure its performance. Third, make sure the vendor is required to handle confidential customer information in the same way you handle it. Fourth, obtain the right to audit the vendor's performance under the agreement. Finally, and perhaps most importantly, your vendor contract should ensure that the vendor has a plan to continue services in the event of an operational failure.

Getting the vendor contract right is of paramount importance. Your ability to monitor your vendors will likely be limited by the terms you agree to in that contract. Accordingly, spend the time, money, and other resources necessary so that the result is a clear set of comprehensive terms outlining the parties' relationship.

Continuing Monitoring of Vendors

Once the ink dries on the contract and the relationship is underway, you should be monitoring your vendor's performance as a means to reduce risk. The contract will be your guide, and should have set the monitoring parameters and performance metrics.

The monitoring process is derived from the information gathered above and is, in a sense, a mere continuation of the other parts of the overall vendor management process. While the inquiries are potentially infinite, some near-universal continued monitoring questions include:

- Has the vendor maintained a healthy financial condition over the time interval?
- Is the vendor following your policies related to critical issues such a confidentiality and security?
- What level of support and service is the vendor delivering?
- Has the vendor experienced significant turnover in employees or management?
- Is the vendor performing as promised?
- Has the vendor received customer complaints?
- What results has the vendor experienced in terms of its testing of business continuity and other contingency plans?

Again, the key here is to have learned everything you might need to know in the first three stages of the process and have them memorialized in the contract. If all that was done satisfactorily, monitoring is largely an exercise in execution.

CONCLUSION

Like it or not, you will find yourself at the intersection of UDAAP and vendor management if you engage vendors to fill out your business lines. The more access you give vendors to your customers, the more access your vendors have to consumer information, and the more likely the intersection may bring risk to your institution. Stay on top of these risks – minimize them – by staying on top of UDAAP and vendor management. It is, simply put, the best way to avoid regulatory intervention.