PUBLICATION

Valuable Information Security Lessons from the Olympus Mortgage vs. Guaranteed Rate Case

April 11, 2016

Late last month a jury awarded Mount Olympus Mortgage Company (MOMC) more than $25 million for their claims against Guaranteed Rate (Guaranteed), which alleged Guaranteed along with other former employees of MOMC illegally transferred hundreds of loan files from MOMC's internal systems to Guaranteed. While the award rightfully highlights some questionable hiring and customer portability issues, it's more notable for showcasing how important it is for a company to maintain control of its data security, both from external threats and employees.

The issue arose when Guaranteed began to solicit two of the country's top producing mortgage loan officers who were then employees of MOMC, along with other MOMC loan officers, for future employment at Guaranteed. According to the complaint filed in June 2014, Guaranteed hatched a "scheme to defraud MOMC of its confidential and proprietary information, including but not limited to proprietary lead sheets, marketing lists, and MOMC forms; as well ***as confidential borrower information, including but not limited to tax returns, social security numbers, pay stubs, addresses, names, and other personally identifiable information*** for the purpose of directing MOMC customers to Guaranteed." In response to these charges the jury ordered Guaranteed to pay more than $25 million in damages to MOMC.

Setting aside the actions of Guaranteed, its executives and the loan officers, the real question is what, if any, steps could have been taken within MOMC to avoid the harm suffered in the first place. The harm is not just lost revenue. In cases like this one, MOMC had to, and will continue to, deal with the reputational repercussions, increased future litigation risk and possible increased compliance risk when they go through their next regulatory exam.

For instance: In addition to Gramm-Leach-Bliley Act (GLBA) requirements imposed on financial institutions to notify individuals of certain "misuse of its information," California law requires a business to notify any California resident whose unencrypted personal information was acquired by an unauthorized person (a version of this law exists in 47 states). Further, any person or business that is required to issue a notification to more than 500 California residents as a result of a single breach of their security system will be required to electronically submit a single sample copy of that security breach notification to the Attorney General. This sample is then posted on a searchable database on the California AG's website. Many AGs have similar requirements and require notice in advance to an AG regardless of the number of individuals affected. The reputational cost of issuing these letters and publishing a sample with the AG can be significant. The letter, in the mind of a customer, may suggest weaknesses in the security of their data and may well sway their opinion when it comes time to obtain another mortgage loan and drive them to a competitor that they have more trust in.

Customers who receive letters like those mentioned above may also blame the data breach for any issues they face with identity theft or any credit issues in the months and years following the breach, unfounded or not. This can result in significant legal spending, as a lender will have to defend against any increase in litigation as result of a breach. Also, a breach can spur a spike in consumer complaints against a mortgage provider, which has a very real cost attached to it as the lender will have to staff and respond to each complaint.

Finally, the Consumer Finance Protection Bureau (CFPB) has stated that they monitor law suits and customer complaints, and then utilize the data as a factor for exam prioritization. Exam prioritization by the CFPB is governed by risk prioritization, and the risk associated with a data breach is an outsized one. The Federal Financial Institutions Examination Council (FFIEC), which the CFPB is a member of, is a formal interagency body empowered to prescribe uniform principles for the federal examination of financial institutions. The FFIEC has stated that an institution should take a "comprehensive approach to maintain the security and resilience of its technology infrastructure including the establishment of a robust cybersecurity framework." They recommend the establishment of "robust governance policies and risk management strategies" and to "commit sufficient resources including expertise and training" as well as the establishment of "an enterprise-wide approach to manage cyber risks with a strong cybersecurity culture as its foundation." As the CFPB is a member of the FFIEC it would be wise to heed the FFEIC guidance.

The CFPB has also shown their ability to bring enforcement actions where they identify data security deficiencies. Although the CFPB lacks authority under GLBA to enforce any of GLBA's data security provisions, they recently utilized their authority under UDAAP to bring an enforcement action against Dwolla, Inc. (a company who operates an online payment platform) for issues with Dwolla's data security policies and procedures. As such, this risk too carries a very real cost.

Cyber security is becoming a larger threat with each passing day. The mortgage industry is particularly susceptible due to the high amount of non-public personal information (NPPI) and automation involved in the processing and underwriting of a home loan. Companies would be best served to review their data protection and privacy policies to ensure they are employing the most recent technology and are consistently revising to compensate for any process breaks that are identified. When conducting a review of relevant data security procedures, be certain to include a security system risk analysis that considers internal risks and any efforts to mitigate those risks. For example:

- Are you controlling access to your origination platform to the positions who actually require access to process your pipeline?
- Are all writable drives removed from your terminals?
- Are email attachments sent from your servers scrubbed for NPPI?
- Does your institution have and enforce a clean desk policy?
- Do you have proper controls over your network access?
- Do you have filters to catch and deny any NPPI being electronically sent outside of your company improperly?
- Are controls in place to prevent any information from being saved on removable drives?

These are questions you should be asking immediately and they are steps your company can take today to guard against data theft. Not to mention these steps will bolster your risk and controls, and look good when built into your compliance management program when it comes time for your next audit. Regular training is also recommended for anyone who handles customer information to remind them of the risk of a data breach and the penalties associated with the misuse of consumer's NPPI. When it comes to privacy and data protection, the best defense is a proactive offense.

In the MOMC matter the loan officers were accused of taking the data to process the borrowers for home loans at Guaranteed. The data breach could have been much worse if the information was taken by a loan officer or processor and simply used as a commodity for sale with the borrower's NPPI utilized for more nefarious purposes such as identity theft. In that case, the liability of the breached entity becomes astronomical – and there would have been no entity to sue to recover a portion of the damages like MOMC did with Guaranteed.

The precautions referenced above may sound like an expensive step to take, but the cost is dwarfed by the price associated with the risks. If you have any questions regarding cyber security or best practices for regulatory exams, please contact any of the attorneys in Baker Donelson's Privacy and Information Security or Financial Services Litigation practice groups.