FDIC Newsletter Highlights Financial Institutions' Cybersecurity Obligations

The FDIC's Winter 2016 edition of its Consumer News publication focuses on how consumers, banks, and regulators can prevent online fraud and theft. *See* FDIC Consumer News Special Edition – Winter 2016: A Bank Customer's Guide to Cybersecurity ("Cybersecurity Guide"), *available at* https://www.fdic.gov/consumers/consumer/news/cnwin16/. The Cybersecurity Guide, which is targeted towards banking consumers, offers a number of tips for how individuals can proactively protect themselves from cybercrime.

In addition, the Cybersecurity Guide offers an overview of the role regulators and banks play protecting consumers' sensitive information. For example, the article "What Banks and Bank Regulators are Doing to Protect Customers from Cyberthreats" highlights the obligations that bank directors and officers owe their customers. *Available at* https://www.fdic.gov/consumers/consumer/news/cnwin16/banks_regulators.html. That article reminds readers that, "[s]ince 2001, federal law and regulations have required that financial institutions have programs to ensure the security and confidentiality of customer information," and that federal and state examiners regularly conduct examinations to ensure that banks are in compliance. The article also points to several ways that banks can work to meet this obligation:

- Banks may "have employees or use outside firms that work to prevent cyberfraud."
- Banks "must continually improve their information security programs so they can effectively respond to the latest cyberthreats."
- Banks may work with regulators "to share overviews of the cyberthreat landscape and discuss steps they can take to be prepared."
- Banks can also "join industry organizations that provide reliable and timely information designed to help institutions protect critical systems from cyber threats."

Although federal law has required banks to protect customers' information since 2001, recent high-profile security breaches have brought increased scrutiny to the cybersecurity of financial institutions. For example, in 2015, a gang of hackers from Russia, Ukraine, Europe, and China infiltrated over 100 banks in 30 countries (including the United States), allowing them to steal over $1 billion over two years. *See* Mike Lennon, "Hackers Hit 100 Banks in 'Unprecedented' $1 Billion Cyber Heist: Kaspersky Lab," Security Week (Feb. 15, 2015), *available at* http://www.securityweek.com/hackers-hit-100-banks-unprecedented-1-billion-cyber-attack-kaspersky-lab. More recently, in January 2016, banking giant HSBC suffered a massive cyber attack. While the bank's security successfully defended the assault, it brought down its online services throughout the United Kingdom. *See* Sinead Cruise, "HSBC says internet banking services down after cyber attack," Reuters (Jan. 29, 2016), *available at* http://www.reuters.com/article/us-hsbc-cyber-idUSKCN0V71BO.

For financial institutions in the U.S., banking regulators offer resources for banks to test the adequacy of their cybersecurity protections. Last July, for example, the FDIC announced that it had developed a Cyber Security Assessment Tool to help financial institutions determine their preparedness for cyber threats. *See* FIL-28-2015 (July 2, 2015), *available at* https://www.fdic.gov/news/news/financial/2015/fil15028.pdf. FDIC examiners will discuss the tool with bank management to raise awareness during subsequent examinations.

Outside consultants can also assist bank management in evaluating their cybersecurity preparedness. Law firms, for example, with experience in directors' and officers' issues could help banks create a response plans and draft internal policies to limit the liability of the banks' management in the event of a cyber attack.

News stories from the past few years and the FDIC's recent Cybersecurity Guide make it clear that banks of all sizes are increasingly vulnerable to cyber attacks, and the directors and officers of financial institutions must protect their customers' sensitive personal information. Through proactive measures taken before a cyber attack occurs, bank management can mitigate the effects of a data breach and reduce their potential future liability.

For more information, please contact:

Dennis Klein, *Partner*
+1 (305) 379-5574
dennis.klein@hugheshubbard.com

Jeffrey Goldberg, *Associate*
+1 (305) 379-5573
jeffrey.goldberg@hugheshubbard.com

Tyler Grove, *Associate*
+1 (202) 721-4625
tyler.grove@hugheshubbard.com

March 2016

Hughes Hubbard & Reed LLP