DREHER TOMKIES LLP

ALERT

FOR CLIENTS AND FRIENDS OF DREHER TOMKIES LLP

December 29, 2014

HOW ARE YOUR CYBERSECURITY PLANS?

On July 17, 2014, the New York Department of Financial Services (NY-DFS) issued for public comment a proposed "BitLicense" regulatory framework for New York virtual currency businesses. *See* our ALERT of August 20, 2014. The comment period ended October 21, 2014. On December 19, 2014, NY-DFS Superintendent Benjamin Lawsky outlined revisions to the proposal during remarks at the Bipartisan Policy Center in Washington. He stated that revised rules will be released in the coming days, after which the public will have 30 days to submit comments. The NY-DFS aims to finalize regulations by early next year.

A common criticism of the proposed framework is that digital money companies will be held to higher standards than those currently applied to financial institutions. In response to the criticism, while speaking at the Cardozo School of Law on October 14, 2014, Lawsky stated that NY-DFS is considering imposing the stronger regulations on banks and insurance companies as well. Specifically, Lawsky suggested that a new cybersecurity regime for banks is in progress. The Office of the Comptroller of the Currency has responded saying that its cybersecurity examinations already are robust for institutions under its authority.

On December 10, 2014, the NY-DFS announced plans to expand its information technology (IT) exam procedures for New York-chartered and licensed banking institutions to focus greater attention on cybersecurity. Future IT/cybersecurity examinations will include, among other topics:

- Corporate governance, including organization and reporting structure for cybersecurity related issues;
- Management of cybersecurity issues, including the interaction between information security and core business functions, written information security policies and procedures, and the periodic reevaluation of such policies and procedures in light of changing risks;
- Resources devoted to information security and overall risk management
- Management of third-party service providers; and
- Cybersecurity insurance coverage and other third-party protections.

The NY-DFS will supplement its pre-examination letters with a separate request for answers to a list of related questions, including background information on the chief information security officer and the entity's due diligence process for vetting, selecting and monitoring third-party service providers.

As a result of recent high profile cybersecurity breaches, such as Target, Home Depot and JP Morgan, cyber threats are a priority for bank regulators. This year, the Federal Financial Institutions Examination Council began a cybersecurity assessment pilot program as part of its regular bank exams. Additionally, President Obama signed an executive order for new initiative "BuySecure" to implement security measures such as microchips and PIN numbers in new and existing government-issued credit cards and card readers for agencies issuing such benefits. He specifically directed the government to "lead by example in securing transactions and sensitive data."

The Gramm-Leach-Bliley Act (the "Act") of 1999 governs bank cybersecurity. The Act requires banks to institute and test an information-security plan, but does not contain specific cybersecurity measures.

The proposed BitLicense framework contains specific cybersecurity rules. Each licensee would be required to establish and maintain an effective cybersecurity program to ensure the availability and functionality of the licensee's electronic systems and to protect those systems and any sensitive data stored on those systems from unauthorized access, use or tampering.

Under the proposed rules, the cybersecurity program must be designed to perform the following five core cybersecurity functions:

- Identify internal and external cyber risks by, at a minimum, identifying the information stored on the licensee's systems, the sensitivity of such information, and how and by whom such information may be accessed;
- Protect the licensee's electronic systems, and the information stored on those systems, from unauthorized access, use or other malicious acts through the use of defensive infrastructure and the implementation of policies and procedures;

Darrell L. Dreher
ddreher@dltlaw.com

Judith M. Scheiderer
jscheiderer@dltlaw.com

Elizabeth L. Anstaett
eanstaett@dltlaw.com

Charles V. Gall
cgall@dltlaw.com

Emily C. Barlage
ebarlage@dltlaw.com

2750 HUNTINGTON CENTER
41 S. HIGH STREET
COLUMBUS, OHIO 43215
TELEPHONE: (614) 628-8000 FACSIMILE: (614) 628-1600
WWW.DLTLAW.COM

To see all previously sent ALERTS, visit our website at www.dltlaw.com

To decline future ALERTS, please contact us at ALERTS@DLTLAW.COM.
This ALERT has been prepared for informational purposes only. It does not constitute legal advice and does not create an attorney-client relationship.

Michael C. Tomkies
mtomkies@dltlaw.com

Margaret M. Stolar
mstolar@dltlaw.com

Robin R. De Leo
robin@dreher-la.com

Susan L. Ostrander
sostrander@dltlaw.com

Susan M. Manship
smanship@dltlaw.com

50546 © 2014 DREHER TOMKIES LLP

- Detect systems intrusions, data breaches, unauthorized access to systems or information, malware and other cybersecurity events;
- Respond to detected cybersecurity events to mitigate any negative effects; and
- Recover from cybersecurity events and restore normal operations and services.

Under the proposed rules, each licensee must implement a written cybersecurity policy which will be reviewed and approved by the licensee's board of directors on at least an annual basis. The written cybersecurity policy must address information security, data governance and classification, access controls, business continuity and disaster recovery planning and resources, capacity and performance planning, systems operations and availability concerns, systems and network security, systems and application development and quality assurance, physical security and environmental controls, customer data privacy, vendor and third-party service provider management, monitoring and implementing changes to core protocols not directly controlled by the licensee and incident response.

The proposed rules require each licensee to appoint a Chief Information Security Officer (CISO) responsible for overseeing and implementing the licensee's cybersecurity program and enforcing the cybersecurity policy. The licensee must also employ cybersecurity personnel adequate to manage that licensee's cybersecurity risk. Each licensee must submit a report to the NY-DFS assessing the integrity of the licensee's electronic systems, identifying relevant cyber risks and proposing strategies for the redress of inadequacies.

Additionally, the proposed rules require each licensee to conduct penetration testing and vulnerability assessment of its electronic systems. The licensee must also maintain audit trail systems and have an independent, qualified third party conduct source code reviews on at least an annual basis.

Financial institutions should keep a close watch on the developing BitLicense rules, specifically as they pertain to cybersecurity, as they are likely to continue to serve as a guide for future regulation. We can assist in reviews of IT/cybersecurity policies. ❑

✧ *Mike Tomkies and Emily Barlage*

As a vendor to financial institutions, their nonbank partners and others in the consumer financial services industry, Dreher Tomkies LLP has always been sensitive to cybersecurity issues. Cybersecurity preparedness and vigilance continue to be a point of emphasis in our IT plans. Our size allows us to remain nimble in addressing emerging issues.

© 2014 DREHER TOMKIES LLP