THREATS AND RISK INSIGHTS

Navigating Cybersecurity Challenges in the Lending Industry

BY RICHARD I. SIMON, ESQUIRE, AND STEVEN W. TEPPLER, ESQUIRE

Attorneys from Mandelbaum Barrett PC explore how the rising cyber threats and stringent regulations facing lenders and the essential strategies for developing robust cybersecurity programs, safeguarding data, and maintaining regulatory compliance in a rapidly changing landscape.

The lending industry, encompassing both traditional banks and non-traditional financial institutions, has become a prime target for cyber-attacks. These attacks range from sophisticated phishing schemes to ransomware assaults, posing significant risks not only to financial assets but also to sensitive customer data. The increasing frequency and severity of these cyber threats have prompted regulatory bodies to impose stringent cybersecurity requirements. Lenders must navigate these regulations to maintain defensible compliance and avoid substantial civil and regulatory penalties.

Challenges Facing the Lending Industry

Evolving Threat Landscape: Cyber threats are continually evolving, with attackers employing increasingly sophisticated techniques. Traditional lenders, such as banks, and non-traditional lenders, including fintech companies, are both at risk. The diversity of these attacks, ranging from data breaches to malware, makes it difficult for lenders to stay ahead.

Complex Regulatory Environment: Lenders must comply with various federal and state regulations designed to protect consumer data and ensure cybersecurity. Key regulations include:

- **Gramm-Leach-Bliley Act (GLBA):** This federal law mandates that financial institutions explain their information-sharing practices to their customers and safeguard sensitive data. Key requirements include developing a comprehensive information security program, conducting risk assessments, and implementing safeguards to protect customer information. Additionally, institutions must provide annual privacy notices to customers and ensure that third-party service providers maintain appropriate security measures.
- **New York Department of Financial Services (DFS) Part 500:** This regulation requires financial services companies to establish and maintain a cybersecurity program designed to protect consumers and ensure the safety and soundness of the state's financial services industry.
- **New York General Business Law (GBL) 899bb:** This statute imposes additional cybersecurity requirements on businesses handling private information.

RICHARD I. SIMON
Mandelbaum Barrett PC

STEVEN W. TEPPLER
Mandelbaum Barrett PC

Resource Constraints: Implementing robust cybersecurity measures requires significant investment in technology, personnel, and training. Smaller lenders, in particular, may struggle with the financial and human resources needed to achieve and maintain compliance.

Data Management Challenges: Lenders handle vast amounts of sensitive customer data, making them attractive targets for cybercriminals. Ensuring the security and integrity of this data while maintaining accessibility for legitimate business purposes is a critical challenge.

Steps to Achieve and Maintain Defensible Compliance

Develop a Comprehensive Cybersecurity Program: Establish a cybersecurity program that addresses the specific risks facing their organization. This program should include risk assessments, regular vulnerability testing, and incident response plans. Under DFS Part 500, for example, financial institutions are required to conduct annual risk assessments and implement a written cybersecurity policy approved by the board of directors.

Implement Robust Data Protection Measures: Protecting sensitive customer data is paramount. This includes encrypting data both at rest and in transit, using multi-

factor authentication, and implementing strong access controls. Compliance with GLBA requires financial institutions to develop, implement, and maintain a comprehensive information security program to protect the confidentiality and integrity of customer information.

Regular Training and Awareness Programs: Employees are often the first line of defense against cyber threats. Regular training and awareness programs can help employees recognize and respond to potential threats. This is crucial for compliance with various regulations, including GLBA, which mandates employee training as part of an institution's information security program.

Third-Party Risk Management: Many lenders rely on third-party vendors for various services, which can introduce additional cybersecurity risks. It is essential to conduct thorough due diligence on third-party vendors and require them to comply with the institution's cybersecurity policies. DFS Part 500, for instance, includes specific requirements for the oversight of third-party service providers.

Continuous Monitoring and Improvement: Cybersecurity is not a one-time effort but an ongoing process. Lenders must continuously monitor their systems for vulnerabilities and update their security measures to address new threats. This proactive approach is necessary to maintain defensible compliance and minimize the risk of cyber incidents.

Employees are often the first line of defense against cyber threats. Regular training and awareness programs can help employees recognize and respond to potential threats. This is crucial for compliance with various regulations, including GLBA, which mandates employee training as part of an institution's information security program.

Engage with Legal and Cybersecurity Experts: *Navigating the complex regulatory landscape* requires specialized knowledge. Lenders should engage with legal and cybersecurity experts to ensure that their cybersecurity programs meet all regulatory requirements and can withstand scrutiny from regulators.

The lending industry faces significant cybersecurity challenges that require a proactive and comprehensive approach to compliance. By developing robust cybersecurity programs, protecting sensitive data, training employees, managing third-party risks, and continuously monitoring and improving their security measures, lenders can achieve and maintain defensible compliance, thereby safeguarding their operations and customer trust.

Richard Simon is a shareholder, co-chair of Mandelbaum Barrett PC's Banking and Financial Services Practice Group, and Partner in Charge of the New York Office. With over 30 years of legal experience, he specializes in commercial lending, including asset-based lending, factoring, trade finance, and finance litigation. Simon advises clients on business structure, planning, finance, corporate governance, cybersecurity, and privacy issues.

He previously served as principal and general counsel for a trade finance company, managing legal affairs and corporate compliance. Simon established the firm's commercial banking finance practice, representing banks and non-bank institutional lenders in loan negotiations and restructuring transactions. He is rated AV Preeminent by Martindale-Hubbell, the highest level of peer-rated professional excellence.

Steven W. Teppler is a partner, chair of Mandelbaum Barrett PC's Privacy and Cybersecurity Practice Group, and Chief Cybersecurity Legal Officer. He focuses on cybersecurity and privacy work, advising on potential class action and mass tort liability related to security vulnerabilities and code defects.

As an ISACA Certified Data Privacy Solutions Engineer (CDPSE), Teppler has been at the forefront of cybersecurity, data privacy, and eDiscovery since 2000. He has extensive experience in technology, blockchain, and class action litigation. Teppler also leads the blog Litigation Intelligence and teaches Electronic Discovery and Cybersecurity Law at Nova Southeastern