New Cyber Risk Reporting Rule

cyber security regulatory

Summary: Due to the high stakes in cyber risks within the financial industry, regulatory agencies recently issued specific guidance called, "Computer Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers." The new rule goes into effect on April 1, 2022, and financial institutions are required to comply by May 1, 2022. Here are the details.

The slogan "*If you see something, say something*" was brought to life as part of a safety and awareness campaign launched by the New York City Metropolitan Transit Authority in 2002 to encourage vigilance among subway and bus riders during their daily travels. But it was initially conceived by an advertising executive named Allen Kay who thought of the slogan the day after the attacks on September 11, 2001, encouraging people to be aware of their surroundings.

Similarly, the banking industry is being asked for its cyber risk vigilance through a new rule in another form of "If you see something, say something." Regulatory agencies have jointly issued the "*Computer Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers,*" with more specific reporting measures. As we reported earlier, the banking industry experienced a 1,318% increase in ransomware attacks alone in just the first half of 2021. Providing effective reporting on cyberattacks is critical in combating them. Here are the highlights of this new rule.

New rule details. The Office of the Comptroller, the Federal Deposit Insurance Corporation, and the Board of Governors of the Federal Reserve System have jointly issued that FIs are required to report cybersecurity incidents to regulators as soon as possible and within 36 hours of being discovered. Under this new rule, FIs must report "significant" cybersecurity issues, such as ransomware or distributed denial of service attacks, so that regulators can get the word out on these industry risks faster. The expedited reporting helps other institutions better secure themselves against the culprits. FIs are also required to inform customers as quickly as possible about any cybersecurity issues that cause problems to their organization for over four hours. **The rule takes effect on April 1, 2021, and FIs are required to be fully compliant with it by May 1, 2022.**

Greater transparency and collaboration. While regulators have long encouraged FIs to be forthcoming about any cyber incidents or risks prior to this new regulation, there was no time requirement for organizations to report these occurrences. The hope is that the new rule will foster greater collaboration between regulators and FIs to more effectively identify and minimize risks that could have a broad-reaching impact on the banking industry. With clearer guidelines on reporting, it should be easier to work together in the fight against cyber thieves to protect financial assets.

Financial institutions actively help. By providing comments to the regulators, FIs were able to help scale back the reach of the final rule, making it more practical. The original version required institutions to report any incidents they "*believe in good faith*" to be cybersecurity threats, instead of incidents confirmed to be legitimate risks. After careful review, the agencies agreed that the "*believe in good faith*" clause was too vague. The final rule notes "*the agencies are replacing the 'good faith belief' standard with a banking organization's determination.*"

FIs are playing a more active role in the fight against cyberattacks in more than one way. Over 240 public and private sector institutions, including FIs, regulators, central banks, information-sharing groups, and law enforcement organizations recently took part in "*Quantum Dawn VI*," a series of simulated ransomware attacks organized by SIFMA, a securities trade group. This event is used to assess the readiness of institutions to respond to the possibility of a widespread ransomware attack on the financial industry. SIFMA has been hosting these preparedness events every 2Ys since 2011.

As the CEO of SIFMA notes in a statement, a "*clear takeaway from the exercise is the importance of a robust partnership between the industry and government grounded in information sharing. No single actor — not the federal government, nor any individual firm — has the resources to protect markets from cyber threats on their own.*"

Working together as an industry to fight the damaging consequences of cybercriminals is ever-more crucial. Hopefully, with the new rule and the ongoing commitment of FIs to stay vigilant on their cybersecurity, we can not only win the battle, but win the war.

TWO APPROACHES TO STRESS TEST YOUR LOANS

Now more than ever, it is important to stress test loans of all types from multiple perspectives. Choose your approach and get expert help, as needed. Learn more about credit stress testing today.

ECONOMY & RATES

Rates As Of: 12/23/2021 07:54AM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	0.08	0.03	-0.01
6M	0.16	0.06	0.07
1Y	0.30	0.05	0.19
2Y	0.70	0.13	0.58
5Y	1.25	0.09	0.89
10Y	1.49	0.04	0.57
30Y	1.89	0.09	0.24

FF Market	FF Disc	IORB
0.08	0.25	0.15

SOFR	Prime	OBFR
0.05	3.25	0.07