Skadden

# Privacy & Cybersecurity Update



## New York Department of Financial Services Issues First-of-Its-Kind Cyber Insurance Risk Framework

**On February 4, 2021, the New York Department of Financial Services (DFS) issued Circular Letter No. 2, which introduced a Cyber Insurance Risk Framework directed to New York-regulated property/casualty insurers that outlines best practices for managing cyber insurance risk. The framework is the first-ever guidance by a U.S. regulator on cyber insurance.**

### Background

In its introduction to the framework, DFS noted that as cybercrime continues to increase for all organizations, cyber insurance is playing an increasingly important role in managing and reducing cyber risk. While cybercrime in general is on the rise, DFS reported that the "biggest driver" of the increase was the frequency and cost of ransomware attacks. According to a 2020 DFS survey, from early 2018 to late 2019 the number of insurance claims that arose from ransomware increased by 180%, and the average cost of a ransomware claim rose by 150% during that same period.

With this in mind, DFS has advised against making ransom payments, as they "fuel the vicious cycle of ransomware, as cybercriminals use them to fund ever more frequent and sophisticated ransomware attacks." In support of this, DFS cited October 2020 guidance from the Office of Foreign Assets Control (OFAC), which stressed the national security risk posed by ransom payments and warned that intermediaries such as insurers can be liable for making ransom payments to sanctioned entities. DFS similarly noted that the Federal Bureau of Investigation warns against making such payments because they do not guarantee that the victim will regain access to the data or that the data will not be publicly released, among other reasons.

### Details of the Framework

To achieve the goal of "foster[ing] the growth of a robust cyber insurance market that maintains the financial stability of insurers and protects insureds," the framework recommends that all authorized property/casualty insurers writing cyber insurance employ the following practices in a manner that is proportionate to their risk:

1. **Establish a formal cyber insurance risk strategy.** The strategy should be directed and approved by senior management and the board of directors (or other governing body) and should incorporate the following six practices identified below.

2. **Manage and eliminate exposure to "silent" cyber risk.** Insurers should manage and eliminate exposure to so-called "silent" (or "non-affirmative") cyber risk, *i.e.*, risk that an insurer must cover loss from a cyber incident under a policy that does not explicitly mention cyber-related coverage, by:
   - identifying exposure to "silent" cyber risk, which "can be found in a variety of combined coverage policies and stand-alone non-cyber policies, including errors and omissions, burglary and theft, general liability and product liability insurance";
   - clarifying whether policies provide or exclude coverage for cyber risk; and
   - taking steps to mitigate existing silent risks, such as by purchasing reinsurance.
3. **Evaluate systemic risk.** Insurers need to assess systemic risk, particularly that posed by third-party vendors such as cloud service providers, and model the effect of catastrophic cyber events, such as self-propagating malware (*e.g.*, NotPetya) and supply chain attacks (*e.g.*, SolarWinds trojan), on these parties. Insurers also should conduct internal cybersecurity stress tests.
4. **Rigorously measure insured risk.** Insurers should conduct data-driven, comprehensive assessments of their (potential) insureds' cyber risks. These assessments should include information gathering on the institution's cybersecurity program through surveys and interviews on topics such as corporate governance and controls, vulnerability management, access controls, encryption, endpoint monitoring, boundary defenses, incident response planning and third-party security policies.
5. **Educate insureds and insurance producers about cybersecurity.** Insurers should educate insureds about cybersecurity and cyber risk mitigation, and incentivize insureds to improve their cybersecurity controls by pricing policies based on cybersecurity program effectiveness. To this end, insurers also should educate insurance producers.
6. **Obtain cybersecurity expertise.** Insurers should recruit employees with cybersecurity expertise in order to properly understand and evaluate cyber risk.
7. **Require victims to notify law enforcement.** Insurers' cyber policies should include a requirement that victims notify law enforcement in the event of a cyber incident, which can help recover funds. In addition, the information received by law enforcement could be used to prosecute the attackers, warn others of existing threats and deter future cybercrime.

### Key Takeaways

The framework is indicative of DFS's continued focus on the critical area of cybersecurity. Although the framework is not binding, New York-regulated insurers' adoption of its best practices may go a long way in effectively managing and reducing cyber risk, improving cybersecurity and ultimately serving DFS's stated goal of facilitating the continued growth of a sustainable and sound cyber insurance market.

Return to Table of Contents

## Eleventh Circuit Holds Future Risk of Identity Theft in Data Breach Suit Does Not Establish Standing

**On February 4, 2021, the U.S. Court of Appeals for the Eleventh Circuit held in *Tsao v. Captiva MVP Restaurant Partners LLC* that a plaintiff had not established standing to sue for a data breach because it failed to demonstrate a substantial risk of future identity theft arising out of unauthorized access to credit card numbers. The court's decision was based in part on the fact that the plaintiff had not provided evidence that any personal information other than credit card numbers had been accessed.**

### Background

On June 22, 2018, PDQ announced that a breach of its point-of-sale system had occurred between May 2017 and April 2018, affecting all PDQ locations in operation, and that as a result of the breach, a third party "m[ight] have accessed" certain personal information of customers, including cardholder names and credit card information. The plaintiff in *Tsao* made at least two food purchases at a PDQ location during the data breach period. Upon learning of the breach, the plaintiff cancelled two credit cards used for his purchases with PDQ. Within two weeks of PDQ's announcement of the data breach, the plaintiff then filed a class action complaint alleging breach of contract, negligence, unjust enrichment and violation of the Florida Unfair and Deceptive Trade Practices Act.

On November 1, 2018, the U.S. District Court for the Middle District of Florida dismissed the plaintiff's complaint for lack of standing, noting that he had failed to allege misuse of the cancelled credit cards, stolen identity or any specific injury in fact suffered as a result of any misuse of customer credit card information. Thus, the District Court held that mere evidence of a data breach was insufficient to establish Article III standing.

The plaintiff appealed the district court's decision in the Eleventh Circuit.

### Eleventh Circuit Decision

In the appeals case, the plaintiff argued two theories of standing: First, that he could sustain future injury from misuse of the personal information that may have been accessed as a result of the breach; and second, that his efforts to mitigate this future risk by cancelling the affected credit cards led to concrete injuries — namely, diminished opportunity for cash back or reward points, the related costs and time and effort spent on cancelling and replacing the affected credit cards, and restricted access to preferred credit cards. The court rejected both arguments.

In rejecting the plaintiff's first argument that a risk of future identity theft establishes standing, the Eleventh Circuit cited Supreme Court rulings in *Clapper v. Amnesty Int'l USA* and *Spokeo, Inc. v. Robins*. In *Clapper*, the Supreme Court held that threatened injury "must be certainly impending to constitute injury in fact," and that "allegations of possible future injury are not sufficient," while in *Spokeo*, the Court held that a concrete injury "must actually exist." In *Tsao*, the Eleventh Circuit noted that while "evidence of actual misuse is not necessary ... to establish standing following a data breach," a named plaintiff in a class action must provide "specific evidence of some misuse of class members' data" to show that there is a "certainly impending" harm of future identity theft or that such harm is of "substantial risk." Because the plaintiff had not provided any such evidence, the court held that evidence of a data breach by itself did not establish standing.

The ruling also was guided by the Eighth Circuit case *In re SuperValu Inc.*, in which the court found that even alleged actual misuse of certain personal information did not establish standing on the basis of an increased risk of identity theft. Both the Eleventh Circuit and the Eighth Circuit also were persuaded by the findings in a 2007 Government Accountability Office report that noted that credit or debit card information alone with no other personal information (such as birthdates and Social Security numbers) "generally cannot be used to open unauthorized new accounts" and that "most breaches ha[d] not resulted in detected incidents of identity theft."

The court also rejected the plaintiff's second argument that his efforts to mitigate the future risk of identity theft caused by the data breach led to concrete injuries. In its ruling, the court cited the Supreme Court's observation in *Clapper* that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." The Eleventh Circuit noted that the injuries the Tsao plaintiff alleged were inextricably tied to his perception of the "insubstantial, non-imminent risk of identity theft."

The Eleventh Circuit's opinion deepened the circuit split as to whether an increased risk of identity theft establishes standing. As the court noted in its opinion, the Sixth, Seventh,[1] Ninth and D.C. circuits[2] have held that an increased risk of future identity theft establishes standing. In December 2019, the Supreme Court of Georgia also ruled that allegations of probable identify theft — short of actual identify theft — were sufficient to state a cause of action under Georgia law.[3] On the other side of the split, the Second, Third, Fourth and Eighth circuits have reached the opposite conclusion.

### Key Takeaways

The Eleventh Circuit's holding in *Tsao* deepened the circuit split on standing requirements in data privacy suits. In circuits in which a greater showing of injury is required, *Tsao* adds to a growing body of evidentiary guidance those courts may deem inadequate to confer standing, including possible unauthorized access only to credit card information without additional personal information (such as birthdates and Social Security numbers).

Return to Table of Contents

## NIST Releases Its Cybersecurity and Privacy Priorities for 2021 and Beyond

**On February 2, 2021, the National Institute of Standards and Technology (NIST) published an article outlining specific cybersecurity and privacy concerns that the consortium will seek to address in 2021 and in years ahead.**

As stated in the article, in the coming years NIST will focus on managing cybersecurity risks in connection with larger enterprise risk, analyzing the intersection between cybersecurity and privacy, delineating the cybersecurity of systems versus components, and actively engage more internationally and in cross-cutting standards work. Specifically, NIST identified nine cybersecurity and privacy goals:

[1] For more on the Seventh Circuit ruling, please see Skadden's May 2020 "Privacy & Cybersecurity Update."

[2] For more on the D.C. Circuit cases, please see our July 2019 "Privacy & Cybersecurity Update."

[3] For more on the Supreme Court of Georgia case, please see our January 2020 "Privacy & Cybersecurity Update."

### Enhancing Risk Management

NIST is working to produce a "coordinated and cohesive portfolio of complementary resources" to be made available to the public in order to advance the NIST Cybersecurity Framework and to allow for improved synergy between NIST's Cybersecurity, Privacy and Risk Management frameworks.

### Privacy

Earlier this year, NIST released a quick start guide to help small- and medium-sized businesses create or improve privacy programs in line with the NIST Privacy Framework. The purpose of this guide is to help organizations with limited resources to "get a risk-based privacy program off the ground or improve an existing one."

### Strengthening Cryptographic Standards and Validation

NIST is investigating new ways to approach encryption and data protection that will defend against quantum computer attacks. In order to further this goal, NIST is hosting a competition "to solicit, evaluate, and standardize lightweight cryptographic algorithms suitable for use in constrained environments." Results of this competition will be leveraged to form the core of the first post-quantum cryptography standard.

### Cybersecurity Awareness, Training, Education and Workplace Development

In conjunction with its National Initiative for Cybersecurity Education, NIST expressed its continuing commitment to facilitating discussions between employers and employees regarding cybersecurity skills and risks.

### Metrics and Measurements

NIST indicated that it will "aim to support the development of technical measurements to determine the effect of cybersecurity risks and responses on an organization's objectives." Further, NIST stated that it will employ the National Vulnerability Database to assign and identify metrics on an industry-by-industry basis.

### Identity and Access Management

NIST plans to review and resolve comments to the Federal Information Processing Standard Publication 201, a U.S. federal government standard that specifies Personal Identity Verification (PIV) requirements for federal employees and contractors. NIST indicated that it will produce a finalized version that will "expand the set of PIV credentials and allow remote supervised identity proofing."

### Trustworthy Networks

NIST identified several ongoing projects related to trustworthy networks in conjunction with its Cybersecurity Center of Excellence, including implementation of IPv6-only enterprise deployment, and 5G and Zero Trust cybersecurity efforts.

### Trustworthy Platforms

NIST held several workshops this year in connection with its development security operations efforts, with plans to integrate security into development operations planning and processes and update existing guidance. In addition, NIST is considering additional projects under the purview of its Cybersecurity Center of Excellence to demonstrate best practices in relation to trustworthy platforms.

### Securing Emerging Technologies

With the goal of ensuring internet of things (IoT) devices are integrated into the security and privacy controls of federal information systems, NIST is looking for public assistance to help guide drafts defining federal IoT cybersecurity requirements.

### Key Takeaways

NIST's goals for the future suggest a robust platform of improving cybersecurity, including cybersecurity of IoT devices. Its guidance will be useful going forward for both small- and medium-sized businesses that often struggle with cyber-related issues, as well as larger companies with more comprehensive programs. We will continue to monitor how these aims are achieved in the coming weeks and months.

Return to Table of Contents

# Privacy & Cybersecurity Update

## Contacts


**Stuart D. Levi**
Partner / New York
212.735.2750
stuart.levi@skadden.com

**James Carroll**
Partner / Boston
617.573.4801
james.carroll@skadden.com

**Brian Duwe**
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

**David Eisman**
Partner / Los Angeles
213.687.5010
david.eisman@skadden.com

**Patrick Fitzgerald**
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

**Todd E. Freed**
Partner / New York
212.735.3714
todd.freed@skadden.com

**Marc S. Gerber**
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

**Rich Grossman**
Partner / New York
212.735.2116
richard.grossman@skadden.com

**Michael E. Leiter**
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

**William Ridgway**
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

**Jason D. Russell**
Partner / Los Angeles
213.687.5328
jason.russell@skadden.com

**David Schwartz**
Partner / New York
212.735.2473
david.schwartz@skadden.com

**Ingrid Vandenborre**
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@skadden.com

**Helena Derbyshire**
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

**Jessica N. Cohen**
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

**Peter Luneau**
Counsel / New York
212.735.2917
peter.luneau@skadden.com

**James S. Talbot**
Counsel / New York
212.735.4133
james.talbot@skadden.com

**Eve-Christie Vermynck**
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com





Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000