Skadden

# Privacy & Cybersecurity Update



## Washington Becomes First US State to Pass Facial Recognition Law

**Washington state became the first state to pass legislation allowing facial recognition to be used by state and local government agencies, with certain limitations.**

On March 31, 2020, Washington state Gov. Jay Inslee signed a bill establishing specific rules governing the use of facial recognition software by state and local government agencies, becoming the first U.S. state to pass a law establishing and limiting the use of this technology. Facial recognition software can identify individuals in photos and videos based on images from a database of known subjects, but while the technology has been lauded for advancing the security and protection of citizens, it also has been criticized by civil rights activists as having the potential to invade people's privacy and exacerbate racial and gender biases. The bill aims to regulate state and municipal government agencies' use of facial recognition services by July 2021.

### Key Aspects of the Law

The state's law requires government agencies to obtain a warrant to run facial recognition scans in the course of an investigation, except in the case of an emergency. Local and state authorities are allowed to use facial recognition in a search for missing persons, in Amber Alerts (for child abduction) and Silver Alerts (primarily used for missing elders), and for public safety. The law requires training of personnel and regular public reporting regarding the use of the technology. Finally, the software that a public agency uses must have a way to be independently tested for "accuracy and unfair performance differences" across skin tone, gender, age and other characteristics.

### Reactions

The American Civil Liberties Union of Washington said it was disappointed in the passage of the legislation and called for a temporary ban on facial recognition technology pending further discussion on whether it should be used at all.

Washington is the first state to legalize the use of facial recognition technology, following citywide bans in San Francisco, Berkeley and Oakland, California, as well as in Somerville, Massachusetts.

### Key Takeaways

The Washington state law is designed to strike a balance between the civil rights issues associated with the use of facial recognition software and the perceived advancements in public safety that the technology could provide. Depending on where each state aligns itself within this debate, this new law could be a model for similar laws in other states.

Return to Table of Contents

## UK Supreme Court Rules Employer Not Liable for Data Breach Caused by Disgruntled Employee; Liability May Apply in Other Contexts

**The U.K. Supreme Court has ruled that an employer cannot be held vicariously liable for a data breach caused by the actions of a rogue employee, but rejected the argument that U.K. data protection law can never give rise to vicarious liability for employers.**

On April 1, 2020, the U.K.'s Supreme Court ruled in *WM Morrison Supermarkets plc v Various Claimants*[1] that WM Morrison Supermarkets (Morrisons) is not vicariously liable for the actions of a disgruntled employee. The case largely turned on the court's interpretation of employer liability law in the U.K., finding that the requirement for a close connection between the wrongful conduct and the ordinary course of the firm's business or the employee's employment was not established. However, the court rejected the argument that U.K. data protection laws do not allow for employer vicarious liability in general, and its ruling makes clear that a different fact pattern could support the claim in future data protection breach litigation.

### Background

In January 2014, a Morrisons senior auditor, Andrew Skelton (Skelton), uploaded the data of 99,998 Morrisons employees to a publicly accessible file-sharing website in an apparent response to a disciplinary action taken by the company against him months earlier. In addition, Mr. Skelton made a copy of the data in the course of gathering it and transmitting it to Morrisons' external auditor. In March 2014, he then sent a CD containing the data to three British newspapers, which alerted Morrisons. The company took steps to remove the data from the internet, initiated investigations and informed the police. Mr. Skelton was arrested and sentenced to eight years in prison.

More than 5,000 of the affected employees brought proceedings against Morrisons on the basis that the company was vicariously liable for Mr. Skelton's conduct and for its own alleged breach of the statutory duty created by Section 4(4) of the Data Protection Act 1998 (DPA),[2] as well as the misuse of private information and breach of confidence.

In the first legal proceeding before the High Court, Morrisons was found to be vicariously liable for Mr. Skelton's breach of statutory duty under the DPA, his misuse of private information and his breach of his duty of confidence, but also found that Morrisons had no primary liability in any of the charges alleged.

The Court of Appeal agreed that the DPA did not exclude vicarious liability for misuse of private information, nor for breach of confidence. The court also found that Mr. Skelton's acts were within the "field of activities" assigned to him and that the relevant facts constituted a "seamless and continuous sequence" or "unbroken chain."[3] Based on those findings, the court held that Morrisons was vicariously liable for Mr. Skelton's wrongdoing.

### Two Questions the Supreme Court Had to Consider

When the case came before the Supreme Court, the court had to consider (1) whether Morrisons was vicariously liable for Mr. Skelton's conduct; and (2) if so, whether the DPA excluded the imposition of vicarious liability for (i) statutory torts committed by an employee data controller under the DPA, and (ii) misuse of private information and breach of confidence.

#### Was Morrisons Vicariously Liable for Skelton's Conduct?

In a recent case involving *Morrisons — Mohamud v. WM Morrison Supermarkets plc* — Lord Roger Toulson summarized two related matters for consideration: (1) the "field of activities" the employer had entrusted to its employee, and (2) whether there was a sufficient connection between the position in which the employee was employed and their wrongful conduct to make it right for the employer to be held liable under the principle of social justice. In *Mohamud*, there was "an unbroken sequence of events," where, following a verbal altercation with a motorist at the kiosk, a gas station attendant followed the motorist to his car, opened the door and ordered him never to return to the gas station before assaulting him. The court found that the order to keep away from the employer's premises was in connection with the business, at which the attendant was employed with the purpose of serving customers. Therefore, the test is "not merely

[1] [2020] UKSC 12.

[2] Section 4(4) of the DPA provided that "it shall be the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller." The DPA transposed Directive 95/46/EC of 24 October 1995 (the Data Protection Directive). The DPA has since been replaced by the Data Protection Act 2018, and the (duties under the) General Data Protection Regulation (Regulation (EU) 2016/679, or GDPR).

[3] *Mohamud v WM Morrison Supermarkets plc* [2016] UKSC 11.

a question of timing or causation," and vicarious liability for wrongdoing by an employee is decided by "orthodox common law reasoning, generally based on the application to each case, in the light of the guidance to be derived from decided cases." [4]

In the recent *Morrisons* case, the Supreme Court found that the disclosure of data on the internet did not form part of Mr. Skelton's field of activities as it was not an authorized act. While there was a close temporal link and an unbroken chain of causation linking the provision of data to Mr. Skelton and his wrongful disclosure of the data, the temporal or causal connection did not satisfy the close connection test. The authorization for Mr. Skelton and the tasks required of him were not connected closely enough to the wrongful disclosure such that he could have been acting in the ordinary course of his employment. The fact that he had the opportunity to commit the wrongful act was not sufficient to warrant the imposition of vicarious liability. The court concluded that Mr. Skelton's wrongful conduct was not so closely connected with acts that he was authorized for, such that, for the purposes of Morrisons' liability to third parties, his conduct cannot fairly and properly be regarded as acting in the ordinary course of his employment.

The court's ruling also appeared to include a departure from the approach in the *Mohamud* case, where the employee's motive in that case was considered to be "irrelevant." The gas station employee's confrontation with the motorist that occurred by his car was a continuation of the argument that had taken place at the sales kiosk. Therefore, the court ruled that the employee had not "metaphorically taken off his uniform the moment he stepped from behind the counter" and was not "pursuing his private ends."

In the *Morrisons* case the court clarified that, in *Mohamud*, Lord Toulson had in fact considered whether the employee was acting for personal reasons but concluded that the incident constituted "a seamless episode" in the course of employment. This was not the case for Mr. Skelton, whose motive was important, as the court ruled he was not acting "about his employer's business," but instead pursuing a personal vendetta in which the employer might be vicariously liable for his wrongdoing, which was designed specifically to harm the employer.

### Does the DPA Exclude the Imposition of Vicarious Liability?

Morrisons argued that the DPA does not allow for the imposition of vicarious liability, but the court found its arguments unpersuasive. Although the DPA included no discussion about the position of a data controller's employer, the court decided that imposing statutory liability on a data controller such as Mr. Skeltonis not inconsistent with the co-existence of vicarious liability of his employer, whether for breach of the DPA at common law or in equity. The court's ruling showed that it is irrelevant that a data controller's statutory liability under the DPA is based on a lack of reasonable care as opposed to vicarious liability for an employee's conduct, which is not based on fault. As such, it makes no difference that an employee's liability may arise under statute instead. Furthermore, the legislation was intended to increase the protection of data subjects rather than take away existing protections.

### Key Takeaways and Implications for Future Data Protection Breach Actions

*Morrisons* suggests that a wrongful action committed for purely personal reasons might not sustain the claim of vicarious liability in the future. However, a different fact pattern and set of reasons for an employee committing data protection breaches could produce a very different outcome in a different case. As Lord Donald Nicholls stated in *Dubai Aluminium Co Ltd v Salaam*, when distinguishing between an employee pursuing his own interests on "a frolic of his own" and "[an] employee … engaged, however misguidedly, in furthering his employer's business," any wrongdoing of an employee potentially construed in light of the latter scenario might increase the risk of successful vicarious liability claims for large-scale data protection breaches.

Furthermore, it is evident that businesses cannot exclude the imposition of vicarious liability as the claim may be based upon statutory or common law wrongs. Although one species of claim may have been excluded in *Morrisons*, there remain many avenues for affected data subjects to pursue claims against employers for a data protection breach. Insurers also will be taking note of this changing landscape.

However, data subjects considering a group or representative action should still proceed with caution. In particular, there has been very limited court consideration of the significance of a loss for claims under the DPA (as well as its successor, the Data Protection Act 2018, and the GDPR). As it stands currently, in *Morrisons* there has not yet been a decision on that issue, so there are no clear guidelines to inform potential future group actions or funders as to how the English courts will quantify compensation and what sort of damages will be awarded. There also may be practical considerations, such as the costs involved in mounting such challenges. The representative action brought by Richard Atkinson against Equifax Limited for the significant cyberattack against Equifax Inc in 2017 was recently withdrawn, with Equifax permitted to recover its costs — a sage reminder that there remains a long way to go for large-scale data protection breach actions in the U.K.

Return to Table of Contents

[4] One recent formulation of what is known as the "close connection" test can also be found in *Dubai Aluminium Co Ltd v Salaam* [2003] 2 AC 366, which was discussed by the court in *Morrisons*.

## New York Department of Financial Services Releases Cybersecurity Guidance in Response to COVID-19

**The New York Department of Financial Services (NYDFS) released guidance for companies within its jurisdiction on how to identify and address mounting cybersecurity risks associated with the COVID-19 pandemic.**

On April 13, 2020, NYDFS published guidance[5] for regulated entities, highlighting heightened cybersecurity risks in light of the impact of the COVID-19 pandemic. The department also reiterated its incident reporting requirements have not changed in spite of the current circumstances, noting that cybersecurity events must still be reported within 72 hours as per usual obligations. The guidance offers recommendations across three areas of increased risk: remote working, phishing and fraud, and third-party risk.

### Risks and Mitigations

#### Remote Working

The increase in people remotely working due to COVID-19 presents additional cybersecurity challenges compared to those in a typical workplace as hardware is significantly more vulnerable when connected to employees' home networks. Justin Shibayama Herring, executive deputy superintendent of the NYDFS Cybersecurity Division, speculated that a significant percentage of personal computers already have been compromised. NYDFS' guidance highlights five areas of concern associated with remote working and offers recommendations companies can use to address these risks.

- Secure Connections: Regulated entities should focus on ensuring remote access is as secure as possible, including by utilizing multifactor authentication and secure VPN connections to encrypt data in transit.
- Company-Issued Devices: All devices used for remote working should be properly secured, including by installing security software and preventing employees from adding or removing applications.
- Bring Your Own Device Expansion: If an expanded Bring Your Own Device policy is necessary to enable remote working, companies should employ additional security measures to mitigate increased security risks.
- Remote Working Communications: Video- and audio-conferencing applications that enable remote working have been increasingly targeted by cybercriminals. NYDFS recommends limiting unauthorized access to these tools and training employees on proper use.
- Data Loss Prevention: Regulated entities should remind employees not to use personal accounts to send nonpublic information.

#### Increased Phishing and Fraud

NYDFS warns that online fraud and phishing attempts have become more prevalent amid the pandemic. The guidance recommends that companies offer additional training and remind employees to be aware of phishing attempts. The department also suggests updating authentication protocols for security exceptions and wire transfers to address risks associated with the reduction of face-to-face interactions. Employees should be aware of who they are interacting with, even in remote working environments.

#### Third-Party Risk

The guidance recommends that regulated entities coordinate with critical vendors to determine how to properly address risks to third-party vendors.

### Broader NYDFS Inquiry

The department's guidance follows its March 2020 industry letter requiring all regulated institutions to submit a COVID-19 preparedness plan to address increases in operational risks, including cyberattacks and fraud. Following the March directive, many regulated entities sought clarification from the NYDFS Cybersecurity Division on the areas currently being prioritized. Accordingly, this new guidance reflects NYDFS' continued focus on the implementation of cybersecurity regulations during the pandemic.

### Key Takeaways

NYDFS-regulated entities should be aware of the increase in cybersecurity risks due to COVID-19, including the risks associated with remote working, phishing and third-party vendors. Companies should consider taking the steps recommended in the guidance to maintain effective cybersecurity during the pandemic.

Return to Table of Contents

[5] The NYDFS guidance is available here.

## The European Commission and European Data Protection Board Offer Guidance for COVID-19 Mobile Applications

**The European Commission (EC) and the European Data Protection Board (EDPB) have offered detailed guidance on the development and use of mobile applications to help fight the COVID-19 pandemic, with an emphasis on privacy and security considerations under EU law.**

On April 14, 2020, the EDPB released a letter (the letter)[6] in response to the EC's guidance on the use of mobile applications to combat COVID-19 (the recommendations).[7] The EC's recommendations provide a "toolbox of measures" to be applied in the use of technology by EU member states in the fight against the pandemic, while the letter welcomes the EC's initiative in developing a pan-European and coordinated approach when using mobile applications for such purposes. Both agencies' releases address the data protection and information security measures that should be contemplated when developing COVID-19 mobile applications, while also both emphasizing that the implementation of the data protection principles under the GDPR remains of paramount importance.

### The Commission's Toolbox

The recommendations establish a common approach "toolbox" for the use of mobile applications and anonymized mobile data to address the pandemic. The toolbox consists of practical measures and envisages a pan-European approach in the fight against the virus, which will involve sharing assessments of effectiveness of COVID-19-related mobile applications, as well as sharing information on the interoperability of such mobile applications across the EU and their compliance with data protection laws. A common scheme for using anonymized and aggregated data will help EU member states:

- model and predict the evolution of the disease;
- monitor the effectiveness of decision-making by member states' authorities; and
- form a coordinated strategy for exiting from the COVID-19 crisis.

#### Data Protection and Cybersecurity Considerations

In developing COVID-19 mobile applications, the recommendations stress the importance of respecting fundamental rights and preventing surveillance or stigmatization, with such mobile applications generally guided by the GDPR data protection principles. In particular, the recommendations set out the principles that should be observed, including:

- using the least intrusive measures possible (*e.g.*, utilizing proximity data and avoiding processing location data or movements of individuals). Anonymized and aggregated data should be used where possible;
- ensuring that there are technical requirements in place for the technologies being used (*e.g.*, Bluetooth Low Energy) to establish device proximity, encryption, data security and storage of data on the mobile devices;
- having effective cybersecurity measures to protect the availability, authenticity, integrity and confidentiality of data;
- having expiration measures in place to ensure that personal data that has been collected is deleted when the pandemic is declared to be under control;
- having appropriate methods of warning people who have been in close contact with an infected person and ensuring that the infected person remains anonymous; and
- having privacy settings (in the mobile applications) spelled out and operational in a transparent manner.

#### Process for Development

The recommendations stress that COVID-19-related mobile applications should strictly limit the processing of personal data for the purposes of combating the pandemic. Developers should ensure, on an ongoing basis, that there are:

- regular reviews to assess the continued need for the processing of personal data; and
- measures are in place to ensure that personal data is irreversibly destroyed once the processing of the data is no longer required.

Development of an app's toolbox should be done while being mindful of the changing circumstances of the crisis and utilize best practices accordingly.

### The EDPB's Letter

#### General Consideration for COVID-19-Related Mobile Applications

In its letter, the EDPB acknowledges that no "one-size-fits-all solution" exists for COVID-19-related app data protection and that technical solutions will need to be examined on a case-by-case basis. The letter suggests that developers of these applications consult with data protection authorities to ensure that personal data is processed in accordance with applicable data protection laws. The EDPB underlines that such mobile appli-

[6] The EDPB's letter is available here.

[7] The European Commission's recommendations are available here.

cations should be developed in an accountable and transparent manner, including by utilizing the implementation of privacy-by-design and privacy-by-default mechanisms as required under the GDPR.

On that note, the U.K. Information Commissioner's Office (the ICO) stated a formal opinion confirming that Google and Apple are being transparent about how their jointly created app technology will operate and are making clear statements on how privacy-by-design features in their work on contact tracing technology will be achieved.[8]

In developing COVID-19-related mobile applications, developers also should conduct data protection impact assessments (DPIAs) to document privacy practices and justifications in light of individuals' fundamental rights and freedoms. The EDPB strongly encourages that DPIAs are undertaken prior to the processing of personal data taking place in such mobile applications, as this will help developers minimize data protection concerns by identifying risks in the implementation of these applications and ensure that appropriate safeguards are in place. For example, DPIAs can help developers understand what data is required and why, ensuring that suitable measures are in place that govern what happens to collected data once it has been processed. This will help, for instance, mitigate against data being processed in a manner excessive to the purpose it was gathered for.

The EDPB also suggests that the source code of such applications should be made publicly available for scrutiny by the scientific community. Currently, the EDPB has not provided further detail as to how such source code should be released for the purposes of protecting intellectual property rights.

### Specific Considerations for COVID-19-Related Mobile Applications

In its letter, the EDPB addresses specific issues related to the use of mobile applications for virus warning and contact tracing purposes, and sets out several key data protection recommendations which are outlined below.

#### Voluntary Adoption and Legal Basis

The letter emphasizes that the use of COVID-19-related mobile applications should be voluntary and that legislative interventions should not push for compulsory adoption, stating that individuals should be free to install and uninstall such mobile applications at will. That said, the fact that these mobile applications should be adopted on a voluntary basis does not mean that consent is the sole legal basis for the processing of personal data. The letter clarifies that public authorities, when acting as data controllers for the purposes of COVID-19-related mobile applications, also may rely on the necessity for the performance of a task for public interest as the legal basis for lawfully processing personal data.[9]

#### Geolocation Tracking

The EDPB stresses that COVID-19-related mobile applications do not require location tracking of individual users. Collecting data on an individual's movements would be contrary to the data minimization principle and also will create security and privacy risks. In its guidance on the use of location data in the context of the pandemic,[10] the EDPB has stated that "large scale monitoring of location between natural persons is a grave intrusion into their privacy." The board has urged that if location data is collected, it must be properly anonymized and its use can only be legitimized by relying on the voluntary adoption by users (*i.e.*, user consent). This reinforces both the letter and the recommendations' guidance that the use of COVID-19-related mobile applications should be voluntary.

#### Storage of Data

The EDPB notes that although both local storage (within individuals' devices) and centralized storage are valid alternatives for storing data (provided that adequate security measures are in place), local storage (*i.e.*, a decentralized solution) is more in line with the data minimization principle. Safeguards and security measures also will need to be in place for any transfers of personal data that is being stored.

#### Quality of Data and Warning

The letter underlines that the quality of the data processed in relation to COVID-19-related mobile applications is crucial for the use of this technology to effectively help fight the pandemic. Developers should work with health care authorities and scientists to identify what would constitute a "contact event," as well as in what cases the event would be shared and the functional requirements of such mobile applications. The letter states that a mechanism should be in place which ensures the accuracy a diagnosis, such as a one-time scannable code provided with the result of a test. Verifying the accuracy of a COVID-19 diagnosis is crucial for safeguarding mobile applications from becoming a social platform for spreading false alarms.

#### Stigmatization

COVID-19-related mobile applications should include anonymization features to avoid stigmatization for potentially infected people. To achieve this, the letter proposes that such

[8] The ICO's opinion is available here.

[9] For more information, see Skadden's mailing "Protecting Lives Without Destroying Jobs — Using Technology To Suppress COVID-19."

[10] The EDPB's guidance on these applications is available here.

applications, when informing a user of a diagnosis (via an in-app notification) should process only random pseudonyms and should not allow for the reidentification of persons (regardless of their COVID-19 status). The EDPB suggests that no directly identifiable data should be stored in users' devices and that data should be deleted as soon as possible.

**Algorithm**

The letter advises that the algorithms used in COVID-19-related mobile applications should be supervised by qualified personnel (*i.e.*, the developer's IT team, together with health care authorities and scientists) to ensure the reduction of false positives. The EDPB warns that the task "to provide advice on next steps" should not be fully automated and suggests that there be a call-back mechanism, through which a person who has been notified by the application can receive information from a human worker on what to do next.

**Data Retention**

The letter supports the EC's recommendations that, following the end of the crisis, COVID-19-related mobile applications should not remain in use and any collected data should be erased or anonymized.

### Key Takeaways

As mobile application developers move forward in utilizing technology to help fight the pandemic, both the letter and the recommendations accentuate that data protection principles under the GDPR must be followed. COVID-19-related mobile applications should function in an accountable and transparent manner, including by incorporating privacy-by-design mechanisms and processing personal data in accordance with data protection laws. Such applications should operate in the least intrusive manner possible and have appropriate cybersecurity measures to protect the integrity and confidentiality of data that is being collected. In addition, the applications should be voluntary, not track the geolocation data of its users (relying on proximity information instead) and entail anonymization features to prevent stigmatization. Developers also will need to give due consideration to ensure that measures are in place to destroy the collected data once its processing is no longer required. Also, COVID-19-related mobile applications will need to be fine-tuned while keeping the latest developments of the crisis in mind.

Return to Table of Contents

## Equifax To Pay Massachusetts $18.2 Million in Data Breach Settlement

**Equifax has agreed to pay $18.2 million to Massachusetts, as well as strengthen the state's cybersecurity practices, as part of a settlement of claims arising from a 2017 data breach.**

On April 17, 2020, Massachusetts Attorney General Maura Healey announced that Equifax Inc. will pay the state $18.2 million as part of a settlement reached between the credit reporting agency stemming from a major 2017 data breach that affected nearly 3 million Massachusetts residents. The settlement agreement, which is one of the largest data protection penalties ever awarded to a state, also requires Equifax to strengthen its cybersecurity practices.

### Background

On September 7, 2017, Equifax announced that hackers had gained access to sensitive personal data of more than 147 million American consumers in a breach that allowed for identity theft and fraud involving Social Security numbers, dates of birth and physical addresses. As a result of this breach, Equifax agreed to pay $575 million as part of a settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau and 48 U.S. states. Massachusetts and Indiana were the only two states not to join the settlement. According to Attorney General Healy, the settlement was not strong enough and would not do enough for Massachusetts consumers. As such, the Massachusetts Attorney General's Office continued to pursue its action against Equifax under the state's consumer protection and data privacy laws,[11] which culminated in the $18.2 million settlement announced this month.

### The Settlement

The funds awarded in accordance with the Massachusetts settlement will go to the state's general fund and the Attorney General's Office. Although the settlement does not include payments or refunds for consumers, it does ensure that Massachusetts residents can seek payment for any identity theft they may suffer from 2017 Equifax breach from a Consumer Restitution Fund of up to $425 million, which was established as part of the $575 million global settlement reached in July 2019. Equifax also is providing all U.S. consumers with six free Equifax credit reports per year through 2026.

[11] For more information regarding the state's action against Equifax, please read Skadden's April 2018 Privacy and Cybersecurity Update.

In addition to the monetary payment, the settlement requires Equifax to implement an information security program to protect the confidentiality of all personal information on its network, under the supervision of a chief information security officer. Equifax also is required to minimize the collection of sensitive data, keep its software up to date, impose regular security, monitoring and testing requirements, and obtain third-party assessments of its safeguards.

### Key Takeaways

As one of the largest penalties ever paid to a single state over a data breach, the amount of the settlement award is an indication that some states will seek substantial damages in their effort to protect their residents' personal information. Accordingly, when summing up her office's position, Healey said the overall message of the settlement is "protect people's data or you're going to pay."

Return to Table of Contents

## International Financial Think Tank Issues Draft Guidance on Cyberattack Responses

**The Financial Stability Board (FSB), an international organization that monitors and recommends policies intended to stabilize the international financial system, has released proposed guidance for responding to and recovering from cyberattacks, reflecting the potential risks of such attacks to the international financial system.**

On April 20, 2020, the FSB released proposed guidance for responding to and recovering from cyberattacks. The guidance, titled "Effective Practices for Cyber Incident Response and Recovery," describes a variety of measures that companies can implement to help address cyberattacks.[12] The FSB intends to publish a final version of the guidance in October 2020 and is inviting comment from the business community until July 20, 2020.

Though the FSB is not a regulatory body, its members include regulators from the largest economies, as well as international standards-setting bodies and other influential international organizations. The organization also makes policy recommendations to regulators and other policymakers that seek to maintain financial stability.

In the guidelines, the FSB recognizes that cyberattacks pose a threat to the stability of the global financial system and reviews a number of incidents in recent years that affected major financial institutions and the ecosystems in which they operate. The guidelines detail a number of potential avenues for such an incident to occur in the future, including outlining the interconnectedness of many financial systems and the reliance on third-party service providers that could also experience attacks. As explained in the guidelines, a cyber incident could cause loss of confidence in a major financial institution or in a particular financial industry, as well as financial losses to the affected institution. Additionally, a major incident that is not properly contained could seriously disrupt financial systems, which could lead to worldwide financial instability.

The FSB's guidance is intended to provide a "toolkit" that individual companies can adapt to their own circumstances, adjusting for size, industry and regulatory environment. The toolkit consists of 46 effective practices for responding to and recovering from cyber incidents, across seven general subject areas:

- **governance**, to address how cyberattack response and recovery is managed;
- **preparation**, to address readiness to respond to an attack if and when one takes place;
- **analysis**, to address a company's ability to understand when an attack is taking place and the potential and actual impact of the attack;
- **mitigation**, to help a company reduce the actual impact of an attack and address the attack quickly to reduce the harm it causes;
- **restoration**, to address the repair and restoration of systems and data after an attack takes place;
- **improvement**, to establish processes to improve a company's ability to respond to and recover from an attack; and
- **coordination and communication**, to encourage coordination with stakeholders to enhance good situational awareness of cyber threats and to enhance the resilience of the system overall.

Within each of these categories, the proposed guidance includes discussion of a variety of different measures and approaches companies could take in relation to that category. For example, in the area of mitigation, the guidance discusses containment of the attack and isolation of affected systems, business continuity measures, and, ultimately, the eradication of malicious code and data that the attackers may have installed.

### Key Takeaways

The FSB's proposed guidance may indicate a movement toward a more cohesive international standard or set of standards for preparing for and responding to cyberattacks. While none of

[12] The FSB's guidelines are available here.

the specific measures identified in the "toolkit" are particularly unusual or novel, the guidance provides a useful single resource for companies seeking to verify that they are taking appropriate steps to prepare for these attacks.

Return to Table of Contents

## Federal Court Holds Phishing Loss Is Not Covered Under Financial Institution Bond

**A federal court in New Jersey recently held that a bank's loss arising from a phishing scheme is not covered under a financial institution bond, ruling on the plain language of the policy of the bond and signifying how courts may analyze phishing claims going forward.**

On February 11, 2020, the U.S. District Court for the District of New Jersey ruled that insurer Great American Insurance Company (Great American) did not owe coverage under a financial institution bond (FIB) issued to its insured Crown Bank JJR Holding Company, Inc. (Crown Bank), for a loss sustained as a result of a phishing scheme.[13]

### The Phishing Scheme

Crown Bank's procedures permit customers to submit wire transfer requests via phone or email. For all such requests, a Crown Bank employee must, among other actions, have the customer sign and return a wire transfer authorization form, and the employee must call the authorized signatory on the account to confirm the validity of the signature on the form.

Jackie Rodrigues, a Crown Bank director who is married to the bank's chairman and CEO, maintained several accounts with her husband at Crown Bank, and the bank had her signature on file. Over the course of two weeks, Crown Bank received 13 wire requests via email from a fraudster impersonating Mrs. Rodrigues directing the transfer of funds to a bank in Singapore. In each case, the request came from the email address "jackiiesumo@gmail.com," which is identical to Mrs. Rodrigues' actual email address but adds a second lower case "i." Each time, the fraudster completed and returned via email a PDF of the wire transfer authorization form, after which a bank employee printed out the PDF and confirmed the signature with the one the bank had on file. Despite indicating on the wire transfer forms that they did so, the employees never called the telephone number in the bank records to confirm that the request did in fact come from Mrs. Rodrigues. By the time Crown Bank detected the scheme, the bank had transferred over $2.7 million in response to the fraudulent requests.

Crown Bank submitted an insurance claim under the FIB, for which Great American denied coverage.[14]

### The Court's Decision

On cross-motions for summary judgment, the court ruled that Crown Bank's loss was not covered under the FIB. The court reasoned that each wire transfer form was transmitted by email, which is a form of electronic transmission and, as such, was not an "Original" document. The court rejected Crown Bank's argument that the printed PDFs were "Original" documents because the express language of the FIB stated that documents transmitted electronically were not originals "even if received and printed." The court also rejected Crown Bank's argument that a PDF could be considered a "first rendering or archetype" within the definition of "Original" and therefore the term is ambiguous and should be construed in favor of coverage. Rather, the court reiterated that under the plain language of the FIB, the definition of "Original" excluded documents transmitted electronically, whether in PDF format or otherwise.

Turning to Rider No. 6, the court focused on the requirement that the wire transfer forms must bear the "signature ... of one other than the person whose name and signature is on file with the Insured." The court then held that because "Mrs. Rodrigues is an authorized signatory, this loss is squarely outside the plain text of the Rider." Moreover, the court observed that Rider No. 6 also requires possession of the "Original" form and that there is no coverage under the extension for this additional reason.[15]

### Key Takeaways

The court's decision in *Crown Bank* illustrates that unambiguous terms of an insurance policy will be interpreted in accordance with their plain meaning, a cardinal rule of contract and insurance policy construction. The decision also serves as an important reminder to policyholders and insurers alike to carefully review the terms of their policies before a loss occurs in order to fully understand the scope of coverage and its limitations.

Return to Table of Contents

[13] *Crown Bank JJR Holding Co. v. Great Am. Ins. Co.*, 2020 U.S. Dist. LEXIS 23136 (D.N.J. Feb. 11, 2020).

[14] Crown Bank also submitted an insurance claim under a Computer Crime Policy (CCP) issued by Great American and separately recovered $1 million under a Bankers Professional Liability Policy issued by another insurer.

[15] With respect to the CCP, the court denied both parties' motions for summary judgment without prejudice and directed the parties to submit further briefing regarding Crown Bank's "objectively reasonable expectations" regarding coverage under the CCP as required by New Jersey law.

# 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

**Amy Park**
Partner / Palo Alto
650.470.4511
amy.park@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

**Jen Spaziano**
Partner / Washington, D.C.
202.371.7872
jen.spaziano@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