CLEARY GOTTLIEB

Cybersecurité: Aspects réglementaires

Amélie Champsaur

5 juillet 2019

Agenda

1. Overview of EU legislation
2. Cybersecurity under the GDPR
   - Data security and breach notification
   - Enforcement and penalties
   - DPA guidance
3. Cybersecurity under the PSD2
   - Data security context
   - Data security overview
   - Regulatory technical standards – status update and key aspects
   - Enforcement and penalties
4. Cybersecurity under U.S. law
   - U.S. Federal Laws and Regulations
   - U.S. State Laws and Regulations
   - The Payment Card Industry Data Security Standard
   - Equifax Case Study

Overview of EU legislation

Overview: The New EU Cybersecurity Regime

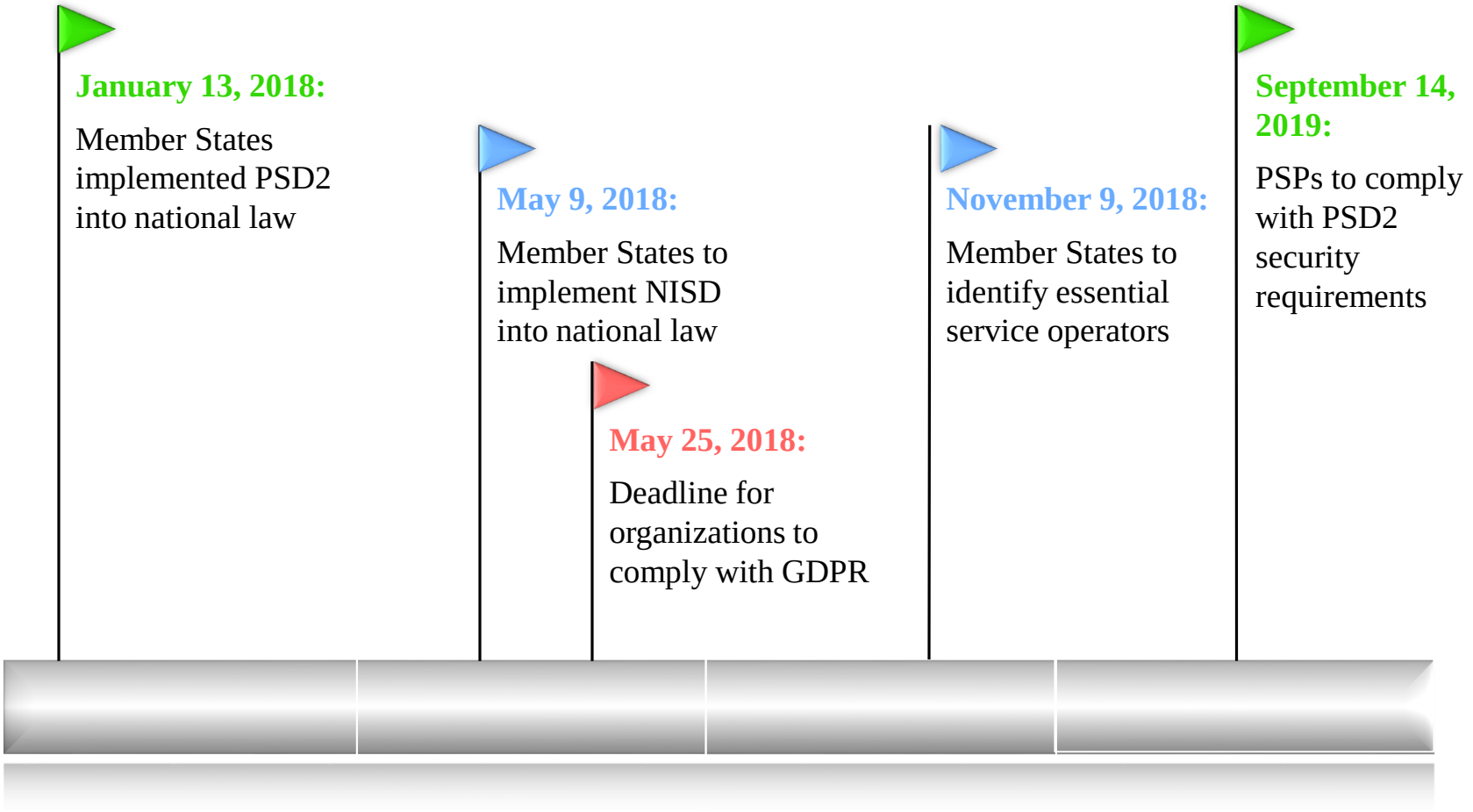
GDPR	PSD2	NISD
—**Policy focus:** Protecting personal data and data subjects. —**Applies to:** All organizations established in, or offering goods or services or monitoring individuals in, the EU (including service providers processing data on behalf of other companies).	—**Policy focus:** Increasing integration, efficiency, innovation and competition across EU payments market, with particular focus on payment security and strong customer authentication. —**Applies to:** Payment, credit and e-money institutions, and providers of payment and account information services.	—**Policy focus:** Network and information security and service continuity. —**Applies to:** *(i)* Organizations identified by Member States as "*essential service operators*" established in the EU (including credit institutions); and *(ii)* digital service providers offering services to persons in the EU.

Brexit and the New EU Regime:

—PSD2 has already been implemented, while GDPR will begin to apply and NISD will be implemented as planned, in the UK.

—Extra-territoriality provisions in all three pieces of legislation will in any event require many UK-based organizations to continue to comply with their requirements post-Brexit.

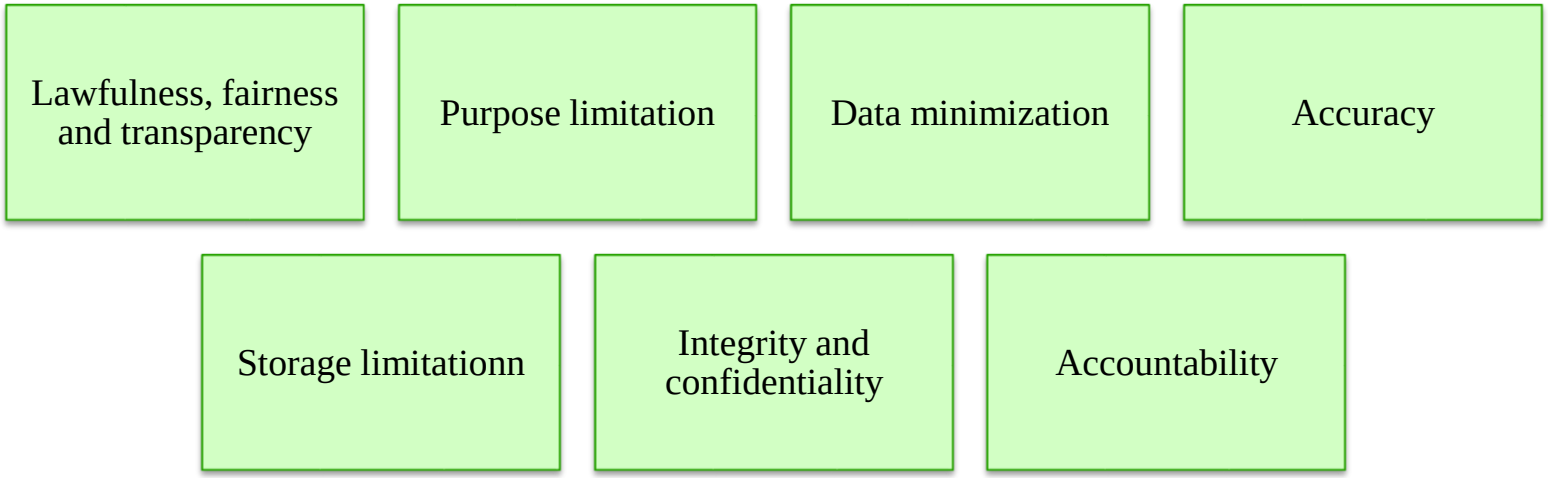
Overview: Implementation of the New Regime – Key Dates



Cybersecurity under the GDPR

GDPR: Key Principles

"*In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States*." (*Recital 10, GDPR*)



GDPR: Key Changes to the Current Regime

- Broder territorial scope
- Data Protection Impact Assessment
- More stringent data security requirements
- Mandatory breach notification (both to DPAs and data subjects)
- Focus on accountability – requirement to demonstrate compliance
- Obligations placed directly on data processors
- Higher penalties
- Greater harmonization between Member States

GDPR: Territorial Scope of the GDPR

— The GDPR applies to:

- The processing of personal data in the context of the activities of an establishment of **a controller or a processor** in the European Union ("**EU**"), regardless of whether the processing takes place in the EU or not; and
- The processing of EU data subjects' personal data by a controller or processor **not established in the EU**, where the processing activities are related to (1) the offering of goods or services to the relevant data subject, or (2) the "monitoring" of the data subject's behaviour, within the EU *(Article 3, GDPR)*.

- Expanded definition of "establishment", based on the case law of the CJEU, *e.g. Google Spain SL, Google Inc. v AEPD, Mario Costeja González (C-131/12)* and *Weltimmo v NAIH (C-230/14)*.
- "EU data subjects" are determined by location in the EU and not by EU citizenship of the individuals.

GDPR: Data Protection Impact Assessment ("**DPIA**")

"*Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.*" *(Article 35, GDPR)*

A DPIA is a process designed to:

— describe the processing;

— verify its necessity and proportionality;

— help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by determining the measures to address them; and

— demonstrate compliace (accountability).

Examples of high risk processing:

— a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling;

— processing on a large scale of special categories of data referred to in Article 9 of GDPR or of personal data relating to criminal convictions and offences;

— a systematic monitoring of a publicly accessible area on a large scale.

GDPR: Focus on Risk

— Data security and breach notification obligations under the GDPR are tied to the risks that data processing activities and personal data breaches pose to data subjects on a case-by-case basis.

— What are the risks?

Loss of control over personal data	Discrimination	Identity theft or fraud	Financial loss
Damage to reputation	Loss of confidentiality of personal data	Unauthorised reversal of pseudonymization	Other economic or social disadvantages

GDPR: Data Security Requirements

"Personal data shall be … processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures." ***(Article 5, GDPR)***

— What is **appropriate** differs on a case-by-case basis depending on:

- The state-of-the-art;
- The costs of implementing security measures;
- The nature, scope, context, and purpose of the processing activity; and
- The severity and likelihood of the risk posed by the processing activity to data subjects.

— The GDPR expressly recommends that organizations consider implementing:

- Pseudonymization and encryption of personal data;
- Measures to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
- Measures to restore availability and access to personal data in a timely manner in the event of a security incident; and
- A process for regularly testing, assessing, and evaluating the effectiveness of the security measures in place.

GDPR: Breach Notification – DPAs

Personal data breach: "*Any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data*".

— Data controllers must notify the relevant DPA **without undue delay** on becoming aware of a breach.

- Notification must be made within 72 hours where feasible.
- A notification made after 72 hours must be accompanied by reasons for the delay.
- The required information can be provided in phases – it is preferable to make an initial placeholder notification within 72 hours, and subsequently follow up with further information as and when it becomes available.

— An **exception** applies when the data controller can demonstrate that the breach is "*unlikely to result in a risk*" to data subjects.

Notification contents:

—Description of the personal data breach, including (where possible) the categories and approximate number of data subjects and personal data records concerned;

—Name and contact details of the data protection officer or other contact person;

—Likely consequences of the breach; and

—Remedial measures taken or proposed to be taken by the data controller.

GDPR: Breach Notification – Data Subjects

— When a personal data breach is likely to result in a "*high risk*" to data subjects, the data controller must notify relevant data subjects **without undue delay**.

— **Exceptions** apply when:

- The affected personal data have been rendered unintelligible by encryption prior to the breach;
- The controller has taken measures after the breach to ensure that the high risk to data subjects is no longer likely to materialize; or
- Individual notification would involve disproportionate effort, in which case data subjects may be notified by means of public communication.

Notification contents (clear and plain language):

—Description of the personal data breach;

—Name and contact details of the data protection officer or other contact person;

—Likely consequences of the breach;

—Remedial measures taken or proposed to be taken by the data controller; and

—Recommendations for the data subject to mitigate possible adverse effects of the breach.

GDPR: Accountability – Demonstrating Compliance

— The GDPR requires organizations not only to comply with its requirements but to be able to **demonstrate compliance**.

— The EDPS has publicly emphasized on several occasions that being able to demonstrate compliance is the most important aspect of GDPR-preparedness.

— How to demonstrate compliance with cyber security measures?

Data Security

— Comply with a code of conduct drawn up by an industry association and approved by a DPA.

— Adhere to an approved certification mechanism, such as ISO 27001.

Breach Notification

— Continue post-notification to document the facts relating to any personal data breach, the effects of the breach, and the remedial action taken, and be able to produce such documentation to a DPA.

GDPR: Controllers and Processors

Data processors have direct statutory liability to:

—Implement appropriate data security measures on the terms as data controllers; and

—Notify personal data breaches to data controller without undue delay.

Data controllers must:

—Only use processors that provide sufficient guarantees to implement appropriate data security measures.

—Undertake thorough diligence of prospective processors, including by auditing the processor or seeing evidence of approved certifications.

—Undertake a Data Protection Impact Assessment prior to entrusting high-risk data to a processor.

—Subject processors to contractual obligations in data processing agreements.

Processor contractual obligations:

—Ensure personnel are subject to confidentiality obligations;

—Have in place appropriate technical and organizational measures to ensure data security;

—Notify data breaches to controller without undue delay and by a specified deadline; and

—Assist and provide all information necessary for controller to comply, and demonstrate compliance with, GDPR requirements.

GDPR: Enforcement and Penalties

DPA Investigative Powers

- To order organizations to provide information.
- To carry out investigations in the form of data protection audits.
- To obtain access to premises, including any means or equipment used for processing personal data.

DPA Corrective Powers

- To order organizations to comply with the GDPR.
- To order a data controller to communicate a personal data breach to a data subject.
- To impose a temporary or permanent ban on processing.

Administrative Fines

- EUR 20 million or 4% worldwide annual turnover for failing to process personal data in a manner that ensures appropriate security.
- EUR 10 million or 2% worldwide annual turnover for breaching granular data security requirements or breach notification requirements.

Private Damages Actions

- Express right for data subjects to be compensated for damage suffered as a result of GDPR infringements.
- All parties responsible for an infringement (whether as data controllers or processors) are jointly and severally liable.

Cybersecurity under the PSD2

PSD2: Data Security Context

"*Security of electronic payments is fundamental for ensuring the protection of users and the development of a sound environment for e-commerce. All payment services offered electronically should be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud.*" *(Recital 95, PSD2)*

- PSD2 builds on PSD1's objectives of making cross-border payments relating to the EU as easy, efficient and secure as national payments within a Member State.
- The Commission acknowledges that the benefits to the European economy that it perceives in maintaining a harmonized payments regime are fundamentally dependent on the security and reliability of payments and accounts information.
- One of PSD2's overarching objectives is to protect consumers against fraud, possible abuses and payment incidents through enhanced security requirements.
- The issue, however, is that PSD2's requirements to provide account access (e.g., through Open APIs) opens up a significantly greater surface area for cyber attack. PSPs may no longer be able to shield off critical internal software and databases behind perimeter IT firewalls.

- **AISP** account information service provider
- **ASPSP** account servicing payment service provider
- **PISP** payment initiation service provider
- **PSP** payment service provider
- **RBA** risk-based authentication
- **SCA** strong customer-based authentication
- **TPP** third party payment service provider
- **TRA** transaction-risk analysis

PSD2: Data Security Overview

Operational and Security Risk Management and Reporting

Payment institutions are required to provide:

- details of procedures in place to monitor and respond to security incidents (Art 5(1)(f));
- a security policy document and detailed security risk assessment, updated at least annually (Art 5(1)(j));
- a report on the adequacy of the control and mitigation measures deployed (Art 95(2)) and statistical data on fraud incidents (Art 96(6)), each at least annually.

Strong Customer Authentication and Secure Communication (SCA)

Subject to specific exemptions, PSPs are required to apply SCA where the payer (a) accesses its payment account online; (b) initiates an electronic payment transaction; or (c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses (Art 97).

Incident Reporting

In the event of a major operational or security incident, PSPs are required to notify the competent authority in the PSPs' home Member State "without undue delay" (Art 96(1)).

- **AISP** account information service provider
- **ASPSP** account servicing payment service provider
- **PISP** payment initiation service provider
- **PSP** payment service provider
- **RBA** risk-based authentication
- **SCA** strong customer-based authentication
- **TPP** third party payment service provider
- **TRA** transaction-risk analysis

PSD2: Regulatory Technical Standards and Guidelines

— On November 27, 2017, the Commission, based on a text submitted by the EBA, adopted Regulatory Technical Standards on SCA that, for the majority of their rules, will apply from September 14, 2019.

— On July 27, 2017 the EBA issued guidelines on major incident response addressed to

- Payment service providers, on the classification of major incidents and on the content, the format and the procedures for notifying such incidents
- Competent authorities, on the criteria on how to assess the relevance of the incident and the details of the incident reports to be shared with other domestic authorities.

— On December 12, 2017 the EBA issued guidelines on the security measures for operational and security risks of payment services

PSD2: Regulatory Technical Standards – Some Key Aspects

Use of Transaction Monitoring Mechanisms (TMMs) to detect abnormal use of credentials, with a risk-based approach using TRA

Security measures must be documented, periodically tested and evaluated by independent and qualified auditors

Exemptions from SCA:

(i) contactless payments up to €50 with cumulative value of € 150 / 5 consecutive payments;
(ii) payments at unattended terminals;
(iii) payments to trusted beneficiaries;
(iv) payments below €30 with cumulative value of €100 / 5 consecutive

PSPs must ensure the confidentiality and integrity of personalized security credentials, including by data masking and encryption.

ASPSPs are primarily responsible for secure authentication. TPPs have the right to rely on the authentication procedures provided by the ASPSP

Authentication codes must be at least 2-factor and may only be accepted once and, for payments, must be dynamically linked to the transaction details

ASPSPs must offer at least one interface for TPP access. TPPs must use an ASPSP's dedicated API if it has one. Screen scraping no longer be permitted

ASPSPs must ensure that any dedicated interface that they provide uses ISO 20022 for financial messaging.

- **AISP** account information service provider
- **ASPSP** account servicing payment service provider
- **PISP** payment initiation service provider
- **PSP** payment service provider
- **RBA** risk-based authentication
- **SCA** strong customer-based authentication
- **TPP** third party payment service provider
- **TRA** transaction-risk analysis

PSD2: Enforcement and Penalties

Authorities' Investigative Powers

— Powers to require provision of information needed to monitor compliance.

— On-site inspections at the payment institution, at any agent or branch providing payment services, or any entity to which activities are outsourced.

Authorities' Corrective Powers

— Suspension or withdrawal of payment institution authorisation.

— Authorities entitled to take steps to ensure payment institution has sufficient capital for payment services.

— Power to share information with other Member State authorities.

Administrative Fines

— To be determined by each Member State.

— Penalties shall be "*effective, proportionate and dissuasive*."

— Administrative fines may be disclosed to the public (unless it would seriously jeopardize financial markets, *etc*.)

Private Damages Actions

— Express right for affected individuals to be compensated by PSPs/ASPSPs for wrongfully non-executed, defective or late executed payments.

— Express right of recourse for PSPs against other PSPs where liability of one is attributable to fault of another.

Cybersecurity in the U.S.

U.S. Federal Laws and Regulations

— U.S. legislative privacy framework is fragmented – there is no comprehensive federal legislation

— Gramm Leach Bliley Act (GLBA) and related regulations (GLBA regulates acts of financial institutions with respect to protection of personal data and privacy):

- Interagency guidelines requires financial institutions to have a **written information security plan** designed to: (1) ensure the security and confidentiality of customer information, (2) protect against any anticipated threats or hazards to the security or integrity of such information, and (3) protect against unauthorized access to or use of such information that would result in substantial harm or inconvenience to any customer.
- Following **an assessment of risks**, security guidelines require a financial institution to manage and control the risk through: (1) the design of a program to address the identified risks, (2) train staff to implement the program, (3) regularly test the key controls, systems, and procedures of the information security program, and (4) develop and maintain appropriate measures to dispose of customer information.
- Under interagency guidance, must maintain an **incident response plan** and, when an institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused.
- **Breach notification** obligations to customers and primary Federal regulator when warranted.

— Section 5 of the Federal Trade Commission Act prohibits unfair or deceptive acts or practices

- This has been enforced against companies that failed to safeguard personal data or comply with posted privacy policies

— SEC and CFTC regulations impose data security obligations on certain covered entities

— SEC focus on cyber-related disclosures for institutions with reporting obligations

SEC Cybersecurity Guidance for Public Issuers

— Existing **disclosure** requirements impose an obligation on companies to disclose cyber-related matters based on generally applicable standards of materiality.

- Companies are expected to provide non-generic disclosure tailored to particular cybersecurity risks and incidents.
  - "For example, if a company previously experienced a material cybersecurity incident involving denial-of-service, it likely would not be sufficient for the company to disclose that there is a risk that a denial-of-service incident *may* occur."
- Companies may have a duty to correct prior disclosure that was untrue (or omitted a material fact necessary to make the disclosure not misleading) at the time it was made or a duty to update disclosure that becomes materially inaccurate after it is made.

— A company's **disclosure controls and procedures** must cover cyber-related matters.

- The controls should not be focused solely on information that relates to disclosure that is required, but should also "ensure timely collection and evaluation of information *potentially* subject to required disclosure, or relevant to an assessment of the need to disclose developments and risks that pertain to the company's business."

— **Insider trading** prohibitions must take into account cybersecurity incidents.

U.S. State Laws and Regulations

— Most states have data breach notification laws (including many that apply regardless of the magnitude of the breach). Failure to comply can result in significant fines (on a per day/per violation basis). Certain states have also imposed data security measures.
  - Some states, but not all, have an exception for entities that are subject to GLBA

— These laws often give State AGs the authority to conduct investigation of cybersecurity practices and to bring enforcement actions on behalf of consumers whose data is breached.

— State AGs, including the NY AG, have shown keen interest in cyber breaches:
  - Target paid $18.5 million to settle state AG investigations
  - Anthem paid $260 million in remediation
  - Multiple AGs have brought actions against Equifax and Uber

NY Department of Financial Services Cybersecurity Regulations (Effective Beginning Aug. 28, 2017)

NY DFS Cybersecurity Regulations applies only to organizations licensed in New York, but the requirements may by predictive of future requirements of other state regulators and is becoming the standard for best practices.

Coverage

- These regulations apply entities operating under a license and/or charter under New York banking, insurance, or financial services laws.
- The NY DFS regulations cover all nonpublic electronic information, even if not personally identifiable or financial information as long as it:
  - Is business-related; and/or
  - Could be combined with other information to identify an individual.

Examples of Obligations

- Implement policies and procedures addressing cybersecurity risk, including mandatory risk assessments
- Designate a qualified individual to act as a Chief Information Security Officer
- Notify DFS **within 72 hours** of any act or attempt to gain unauthorized access to, or to disrupt or misuse an organization's information system
- Document all information relevant to cybersecurity program and make such information available upon request to DFS.

Payment Card Industry Data Security Standard (PCI DSS)

- PCI Security Standards Council was founded in 2006 by the major card brands to implement requirements designed to ensure that all organizations that store, process, or transmit cardholder data do so in a secure environment.
- PCI DSS is a core set of best data security practices that covered organizations must follow to remain PCI compliant:
  - Set of 12 requirements broken down into 6 categories, as follows:
    1. Build and maintain a secure network
    2. Protect cardholder data
    3. Maintain a vulnerability management program
    4. Implement strong access control measures
    5. Monitor and test networks
    6. Maintain an information security policy
- Validation of compliance is performed annually, either by an external Qualified Security Assessor (QSA) or by a Internal Security Assessor (ISA) that creates a Report on Compliance for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes.

Enforcement and Litigation Trends

— Enforcement

- SEC appears primed to bring additional enforcement actions.
- FTC authority to bring enforcement actions is being challenged.
- State authorities, such as NY DFS, will continue to be aggressive (potential "broken windows" theory of enforcement).
- More states are imposing data security requirements on top of breach notification obligations.
- Potential for a national federal data breach notification statute.

— Litigation

- Question whether individuals must suffer actual injury in consumer cases.
- Plaintiffs' law firms are now regularly bringing Exchange Act securities class actions after major breaches at public companies ("stock drop" cases).
- Shareholder derivative cases have met limited success to date but Equifax may break the mold.
- Ongoing challenges to attorney-client privilege in incident response context.

U.S. Case Study

EQUIFAX

— In May-July 2017, hackers infiltrated Equifax's systems and stole PII of up to 148 million people (over 40% of the U.S. population).

— Equifax indicated breach occurred because of an unpatched software flaw, blaming a single IT employee who allegedly failed to ensure the implementation of the software patch.

— Following discovery of the breach, but prior to public announcement, the CFO and three other executives sold Equifax shares.

FALLOUT

— Immediate fallout from the breach included more than a **30% drop** in stock price and a loss of approximately **5 billion dollars** in market cap, followed by the **resignation** of Equifax's CEO.

— **Insider Trading Investigations and Charges**: The SEC and DOJ are leading federal probes into whether the four executives violated insider trading laws. One of the executives was formally charged by both agencies in March 2018.

— **Congressional Hearings and Reputational Harm**: Former CEO testified before Congress. Lawmakers from both parties criticized the company. At least one questioned Equifax's continued role in the financial system.

— **State Actions**: Enforcement actions by state attorneys general for violation of data breach notification statutes, which include potential civil penalties of **thousands of dollars per violation**.

— **Consumer Litigation**: Dozens of putative class actions against Equifax demanding **tens of billions of dollars**.

— **Shareholder Litigation**: Various shareholders also brought lawsuits against Equifax and certain officers and directors.

Appendix

GDPR, PSD2 and NISD – A Comparative Breakdown (1)

	GDPR	PSD2	NIS Directive
Data Security Obligation	Implement appropriate technical and organizational measures to ensure personal data are protected against unauthorised or unlawful processing, accidental loss, destruction, or damage. Use only third party processors providing sufficient contractual guarantees to do the same.	The RTS for SCA contemplate detailed data security obligations. More broadly, all payment services offered electronically should be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud.	Take appropriate and proportionate technical and organizational measures to ensure network and information systems can resist actions compromising the availability, authenticity, integrity, or confidentiality of data stored, transmitted or processed by, or services offered by or accessible via, such systems.
Service Continuity Obligation	Implement measures to restore availability and access to personal data in a timely manner in the event of a security incident.	Establish a framework with appropriate mitigation and control measures to manage operational and security risks, including taking all reasonable steps to ensure continuity and reliability in the performance of payment services.	Take appropriate measures to prevent and minimise the impact of security incidents to ensure service continuity.
Breach Notification Trigger (Relevant Authority)	A breach of security leading to the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data, unless the breach is unlikely to result to a risk to individuals.	A major operational or security incident.	Any event having an actual adverse effect on the security of network and information systems, and which has a significant impact on service continuity.
Notification Deadline (Relevant Authority)	Without undue delay upon becoming aware of the breach and within 72 hours when feasible.	Without undue delay.	Without undue delay.

GDPR, PSD2 and NISD – A Comparative Breakdown (2)

	GDPR	PSD2	NIS Directive
Notification contents (Relevant Authority)	Description of the breach (including categories and approximate number of data subjects and personal data records concerned), contact details, likely consequences of the breach, and remedial measures taken or proposed to be taken.	Collect all relevant information by completing the template provided under the RTS in an incremental manner, on a best effort basis, as more information becomes readily available in the course of their internal investigations. Furnish any additional information by appending supplementary documentation to the standardised template. Payment service providers should deliver the final report when the root cause of the analysis has taken place, in any event within a maximum of 2 weeks after business is deemed back to normal. Payment service providers should aim to include in their final reports full information.	Information enabling the authority to determine any cross-border impact.
Breach Notification Trigger (Affected Individuals)	A breach that is likely to result in a high risk to individuals.	A major operational or security incident that has or may have an impact on the financial interests of its payment service users.	The authority may inform the public when public awareness is necessary to prevent or address a security incident.
Notification Deadline (Affected Individuals)	Without undue delay.	Without undue delay. Initial report to the competent authority to be sent within 4 hours from the moment the major operational or security incident was first detected.	N/A
Notification Contents (Affected Individuals)	Description of the breach, contact details, likely consequences of the breach, remedial measures taken or proposed to be taken, and recommended actions the data subject should take. Notification to be in clear and plain language.	Details of the incident and of all measures that they can take to mitigate the adverse effects of the incident.	N/A