Global Investigations Review

The Guide to Cyber Investigations

Editors
Benjamin A Powell and Jason C Chipman

Second Edition

The Guide to Cyber Investigations

Editors:

Benjamin A Powell

Jason C Chipman

Reproduced with permission from Law Business Research Ltd
This article was first published in June 2021
For further information please contact Natalie.Clarke@lbresearch.com

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL, UK

www.globalinvestigationsreview.com

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as at May 2021, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to: natalie.clarke@lbresearch.com.
Enquiries concerning editorial content should be directed to the Publisher:
david.samuels@lbresearch.com

ISBN 978-1-83862-595-5

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ANDERSON MORI & TOMOTSUNE

BAKER MCKENZIE

BCL SOLICITORS LLP

CLIFFORD CHANCE US LLP

COVINGTON & BURLING LLP

CRAVATH, SWAINE & MOORE LLP

RICHARD DENATALE

HUGHES HUBBARD & REED

K&L GATES LLP

KROLL, A DIVISION OF DUFF & PHELPS

BRIAN MCDONALD

QUINN EMANUEL URQUHART & SULLIVAN, LLP

ROPES & GRAY LLP

WILMER CUTLER PICKERING HALE AND DORR LLP

Publisher's Note

The Guide to Cyber Investigations is published by Global Investigations Review – the online home for all those who specialise in investigating and resolving suspected corporate wrongdoing.

It aims to fill a gap in the literature and provide an in-depth guide to every aspect of preparing for and dealing with data breaches and other cyber incidents. These incidents can be challenging, to say the least.

As such it is a companion to GIR's larger reference work, *The Practitioner's Guide to Global Investigations* (now in its fifth edition), which walks readers through the issues raised, and the risks to consider, at every stage in the life cycle of a corporate investigation, from discovery to resolution.

The Guide to Cyber Investigations takes the same holistic approach, going through everything to think about before, during and after an incident. We suggest both books be part of your library – *The Practitioner's Guide* for the whole picture and *The Guide to Cyber Investigations* as the close-up.

The Guide to Cyber Investigations is supplied to all GIR subscribers as a benefit of their subscription. It is also available to non-subscribers in online form only, at www.globalinvestigationsreview.com.

The publisher would like to thank the editors for their energy and vision. We collectively welcome any comments or suggestions on how to improve it. Please write to us at insight@globalinvestigationsreview.com.

Contents

Part I

A 'Typical' Cyber Investigation

4

Regulatory Compliance in the Context of a Cross-border Data Breach

Evan Norris, David M Stuart and Richard J Stark[1]

With the growing awareness of the vast amounts of personal data residing in the cloud, and the sophistication of those who wish to access it, comes an increasingly complex multinational regime of data protection laws with which global organisations must contend. While these laws share many common features, the sheer number of them – and the differences in definitions, standards and exceptions between them – presents a challenge when a data breach occurs. Perhaps most notably, the victim of the breach must adhere to regulatory deadlines in an environment of factual uncertainty that characterises the initial days following a breach. Where a significant number of individuals are affected, achieving regulatory compliance is an ever-increasing challenge for any organisation that does business across borders.

As discussed elsewhere in this Guide, one aspect of a breach investigation for an organisation is to assess early whether the breach raises notification obligations and, if so, in what jurisdictions. While a well-drawn incident response plan will have provided a head start on that assessment, one early aim of the investigation will be to complete the assessment by a careful review of the facts of the breach. In this chapter we provide an overview of the factors that bear on that assessment, as well as some considerations regarding the provision of notification itself. We then provide some observations about the broader data security compliance and enforcement landscape more generally, as we look to a future in which large-scale, cross-border breaches become increasingly commonplace and more and more data regulators and law enforcement authorities have the budgets and experience to address them.

1 Evan Norris, David M Stuart and Richard J Stark are partners at Cravath, Swaine & Moore LLP. The authors wish to thank Cravath associates Shanique C Campbell and Trevor H O'Bryan for their contributions to this chapter.

Determining whether and in what jurisdictions a data breach gives rise to notification obligations

Data breach notification laws across the globe reflect a mix of rules, standards and approaches. In the European Union, the General Data Protection Regulation (GDPR) imposes breach notification obligations that apply broadly to all data controllers and processors,[2] while France and other individual EU Member States maintain additional notification laws that apply more narrowly to specific industry sectors.[3] In the United States, each of the 50 states (as well as most districts and territories) has its own breach notification law, while a number of federal laws (and even some more state laws) regulating different industry sectors also contain breach notification rules for reporting incidents involving medical, financial and other types of data. In total, such rules have been adopted in approximately 130 countries, including jurisdictions throughout Asia, the Middle East, Africa, Latin America and other regions.[4]

These laws differ in myriad ways, including in the scope of their application, how they define a breach, the level of harm that triggers notification requirements, what exceptions may apply, who is notified, who does the notifying and what regulatory penalties may be imposed for noncompliance.[5] In the context of a cross-border data breach, the challenge this variability poses for organisations is particularly significant.

Identification of applicable laws

Data protection laws may apply based on different factors, such as the organisation's method of data collection, the industry in which the organisation operates and the residence of affected individuals.

In the United States, while there is no comprehensive data protection regime at the federal level, a handful of federal laws regulating various industries, including telecommunications, financial services and healthcare, include breach notification provisions that apply primarily based on the type of personal data a regulated entity may collect. For instance, the Gramm-Leach-Bliley Act imposes breach notification obligations on financial institutions, including federally chartered US banks and federal branches and agencies of foreign banks, with respect to non-public customer personal information.[6] Such laws also exist at the

2 'Processing' of data generally refers to the act of performing operations on personal data, including collection, storage and destruction, as well as analytics and alteration. A data 'controller' is an individual or organisation that determines the purpose and means of processing personal data, and a 'data processor' is an individual or organisation that processes data on behalf of the controller (e.g., payroll vendors and data warehouses). *See* GDPR, Article 4.

3 See, e.g., France Data Protection Act of 1978, Article 34 (data breach notification requirements specific to electronic communications services providers).

4 See David Banisar, 'National Comprehensive Data Protection/Privacy Laws and Bills 2020' (15 December 2020), https://ssrn.com/abstract=1951416.

5 The range of potential penalties differs widely between jurisdictions. In the EU, data protection authorities may impose administrative fines for breach notification violations equal to the higher of €10,000,000 or 2 per cent of any organisation's annual worldwide revenue. *See* GDPR, Articles 33, 34, 83(4). By contrast, in Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) caps the fine regulators can seek to impose on organisations that knowingly violate breach notification requirements to US$100,000 CAD. See PIPEDA, S.C. 2000, Chapter 5, Section 28.

6 15 U.S.C. §§ 6801(a), 6805(a).

state level. In New York State, for example, the Department of Financial Services enforces a cybersecurity regulation notification requirement that applies to financial service companies, including insurance companies and both domestic and non-US banks operating within the state, with respect to material business information and some personally identifying individual data.[7] In some instances, compliance with industry specific notification requirements in a federal statute will exempt an organisation from compliance with the requirements of a state's general breach notification law.[8] Outside the industry specific context, US states have consumer-oriented breach laws that typically apply broadly to organisations whenever a security incident involves data belonging to that state's residents. California's breach notification law, for instance, imposes obligations on any person or entity that conducts business in California and holds computerised personal information belonging to California residents.[9] In other words, depending on the type of data compromised in a breach, an organisation may have notification obligations under any number of US federal and state laws.

While many countries' breach laws are similar in scope to US laws, some apply regardless of industry sector and residence of affected individuals. The GDPR's data protection and breach regulations apply to data controllers and processors that maintain an establishment in the EU or conduct processing activities, wherever conducted, that are related to offering goods or services to data subjects in the EU or to monitoring those subjects' behaviour in the EU.[10] The post-Brexit data privacy laws in the UK – the Data Privacy Act of 2018 and the UK GDPR – are effectively identical in substance to the GDPR with respect to the obligations imposed on controllers and processors. And the data privacy laws of several other countries also mirror the GDPR, including, notably, Brazil's data protection regime, the LGPD, which went into effect in August 2020.[11]

Definition of 'personal information'

Many breach notification laws limit the definition of 'personal information' (or some analogous term) to an enumerated list of data characteristics that are considered sensitive. For example, many US state breach laws narrowly define personal information as an individual's first name (or first initial) and last name combined with any other data elements, such as a social security or driver's licence number.[12] California is among other states that apply a somewhat broader definition that covers 'any information that identifies, relates to, describes, or is capable of being associated with, a particular individual', including identifiers such as

7 See 23 CRR-NY 500.01(c), 500.02. New York also passed, in July 2019, the Stop Hacks and Improve Electronic Data Security (SHIELD) Act, which amends and extends data security and breach notification requirements for companies that collect information on New York residents. See N.Y. Gen. Bus. Law § 899-bb.

8 See, e.g., Va. Code Ann. § 18.2-186.6(G) (Virginia breach notification statute granting safe harbour for organisations already subject to the Gramm-Leach-Bliley Act).

9 Cal. Civ. Code §§ 1798.80(a),1798.82 (a)(1).

10 GDPR, Article 3. Under the GDPR, a 'data subject' is 'an identified or identifiable natural person,' and 'an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.' GDPR, Article 4.

11 Lei Geral de Proteção de Dados (LGPD), Law No. 13,709, Section 3.

12 See, e.g., Md. Code Ann., Com. Law § 14-3501(e)(1); Del. Code Ann. tit. 6 § 12B-101(7).

name, signature, address, employment, social security number, bank account number, and credit or debit card number.[13] And to take a US federal example, the Communications Act of 1934 protects 'customer proprietary network information', defined as information relating to the 'quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier'.[14]

By contrast, some breach notification laws adopt far more expansive definitions of personal information that cover any information relating to natural persons. For instance, the GDPR broadly defines 'personal data' as 'any information relating to an identified or identifiable natural person'.[15] Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) provides that 'personal information means information about an identifiable individual'.[16] Such general definitions could extend to almost any information relating to an individual, whether alone or combined with other data elements possessed by an organisation.

Definition of 'data breach'

Across jurisdictions, the definitional elements of a 'data breach' often include one or more of the use, disclosure, acquisition of, or access to data through illegal or unauthorised means.

Many US states define a data breach as the unauthorised or illegal acquisition of personal information.[17] In contrast, some jurisdictions consider unauthorised access, alone or in combination with another activity or a certain result, sufficient to constitute a breach. Under Singapore's data privacy statute, for example, a data breach broadly includes any 'unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data', regardless of whether any harm or risk of harm was caused by the breach.[18] A few US states also define a breach as simply unauthorised access to personal information, whereas others require that the unauthorised access compromises the security, confidentiality or integrity of protected personal information.[19]

Some jurisdictions incorporate a risk standard into the definition of a data breach. For instance, Australia's mandatory Notifiable Data Breach Scheme defines an 'eligible data

13 See, e.g., Cal. Civ. Code § 1798.80(e). Alternatively, some states define personal information as 'any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person'. See, e.g., N.Y. Gen. Bus. Law § 899-aa(1)(a).

14 47 U.S.C. § 222(h)(1).

15 GDPR, Article 4(1). Back in the United States, Virginia recently enacted a comprehensive data protection law (effective January 2023) that echoes the GDPR in broadly defining 'personal data' as information that is 'linked or reasonably linkable to an identified or identifiable natural person'. See Consumer Data Privacy Act § 59.1-571 et seq. Notably, Virginia's older breach notification law defines personal data more narrowly. See Va. Code Ann. § 18.2-186.6(A) (defining 'personal information' as 'the first name or first initial and last name in combination with and linked to any one or more . . . data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted').

16 PIPEDA, S.C. 2000, Chapter 5, Section 2(1).

17 See, e.g., AS § 45.48.090(1); IN §§ 24-4.9-2-2(a).

18 Personal Data Protection (Amendment) Bill 2020, Section 26A.

19 Compare Fla. Stat. § 501.171(1)(a) (defining 'breach' as the 'unauthorised access of data in electronic form containing personal information') with Kan. Stat. Ann. § 50-7a01(h) (defining 'breach' as 'unauthorised access and acquisition of unencrypted or unredacted computerised data that compromises the security, confidentiality or integrity of personal information').

breach', in relevant part, as (1) any 'unauthorised access to, or unauthorised disclosure of, the information' or (2) 'information [that] is lost in circumstances where' unauthorised access or disclosure 'is likely to occur', both of which 'would be likely to result in serious harm to any of the individuals to whom the information relates'.[20]

As security incidents increase in sophistication, the definition of a data breach continues to evolve to include wide-ranging activities in addition to acquisition, access, use or disclosure. This evolution is noticeable in the GDPR's definition of a data breach as any 'accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.[21]

Exceptions and exemptions

Once an organisation determines that a breach of protected personal information has likely occurred, it must evaluate whether any exceptions or exemptions apply that could obviate the need to make a breach notification.

Encryption

Some breach notification laws carve out safe harbours for personal information or data that is encrypted (or substantially redacted) at the time of a breach. While the GDPR does not have an encryption exception, it treats 'state of the art' encryption as a data protection measure that reduces risk to individuals' rights and freedoms,[22] which could potentially excuse an organisation's duty to notify affected individuals.[23] Several US state breach laws, in contrast, explicitly distinguish between encrypted and unencrypted information when defining a data breach of personal information.[24] Some states completely exempt organisations from giving notice to affected individuals so long as the encryption was not compromised in the security incident.[25] In other states, encrypted data elements may be excluded from the legal definition of personal information or data, and the security incident that impacts encrypted data elements may be excluded from the legal definition of a data breach.

Good faith exemption

Notably, some breach notification laws exempt from the definition of a breach certain good faith access or acquisition of personal information by a company employee or agent. For

20 The Privacy Act 1988, § 26WE(2).

21 GDPR, Article 4(12). A few U.S. federal regulations adopt a comparatively broad definition, including the Veterans Affairs Information Security Act, which defines a data breach as 'the loss, theft, or other unauthorised access, other than those incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data.' 38 U.S.C. § 5727(4).

22 GDPR Article 32(1)(a).

23 See id.; GDPR, Article 33(1).

24 See, e.g., Cal. Civ. Code § 1798.82(a); Tex. Bus. & Com. Code Ann. § 521.053(a) (both requiring notification of a breach of encrypted personal information if the encryption key is also acquired).

25 See, e.g., D.C. Code § 28-3851(1)(B)(ii) ('The term 'breach of the security of the system' does not include . . . [a]cquisition of data that has been rendered secure, including through encryption or redaction of such data, so as to be unusable by an unauthorised third party unless any information obtained has the potential to compromise the effectiveness of the security protection preventing unauthorised access.').

instance, under the US Health Insurance Portability and Accountability Act (HIPAA), a data breach does not include 'any unintentional acquisition, access, or use of protected information' by employees of covered healthcare entities if 'made in good faith and within the scope of authority and does not result in further use or disclosure'.[26] Several US states, such as California and Virginia, also recognise a good faith exemption if an employee or agent acquires personal information for a legitimate business purpose and does not make further unauthorised disclosure of the personal information.[27] No similar exemption exists under the GDPR. Brazil also does not recognise a good faith exemption, but 'good faith of the offender' will be taken into consideration to determine appropriate administrative sanctions for data processors that violate the country's data protection law.[28]

Harm thresholds as notice triggers

Several jurisdictions have adopted data breach notification laws that utilise harm thresholds as notice triggers, whereby organisations need only give notice if harm occurred or there is a potential of harm or risk to the individuals whose personal information is breached. Notification laws in several US states enumerate the various types of harm that could trigger mandatory notification requirements, including misuse of personal information,[29] identity theft, fraud or other illegal use of personal information[30] and substantial economic loss or financial harm.[31]

More than half of the US states adhere to harm thresholds in their breach notification laws, but there is variance among the statutes with respect to the risk a breach must present to the resident consumers of those states (the typical group entitled to notice) to require notification. For example, Virginia's breach notification statute requires notification to the state Attorney General and any affected individual if there is a reasonable belief that the breach 'has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth'.[32] Florida, on the other hand, does not require notice to individuals if, after appropriate investigation and consultation with federal, state and local law enforcement, the organisation determines that the breach 'will not likely result in identity theft or any other financial harm'.[33] Florida also does not require notification to its data regulator if fewer than 500 Florida residents are impacted by a breach.[34]

Harm thresholds are also used outside the United States. Under Canada's data privacy law, for example, notification to individuals and the regulator is required only where the breach creates 'a real risk of significant harm to an individual'.[35] Mexico's data privacy law requires that the breach 'significantly prejudice the property or nonpecuniary rights of the

26 45 C.F.R. § 164.402(1)(i), (iii).

27 See Cal. Civ. Code § 1798.82(g); Va. Code Ann. § 18.2-186.6(A).

28 Lei Geral de Proteção de Dados (LGPD), Law No. 13,709, Section 52, § 1(II).

29 See, e.g., Md. Code Ann., Com. Law § 14-3504(b)(2); N.J. Stat. Ann. § 56:8-163(a).

30 See, e.g., VA. Code Ann. § 18.2-186.6(A), (B); N.Y. Gen. Bus. Law § 899-aa(1)(c), (2)(a).

31 See, e.g., Ariz. Rev. Stat. § 18-552(J); Iowa Code Ann. § 715C.2(6).

32 Va. Code Ann. § 18.2-186.6(A), (B).

33 Fla. Stat. § 501.171(4)(c).

34 id. at § 501.171(3)(a).

35 PIPEDA, S.C. 2000, Chapter 5, Section 10.1(1).

data subjects' to require notification to individuals.[36] And the GDPR requires notification to the relevant supervisory authority if the breach presents a 'risk to the rights and freedoms of natural persons' and to individuals if the breach presents a 'high risk' to the same.[37] These differences in statutory definitions of the harm threshold may result in a determination, for instance, that a data breach occurred that was likely to result in a 'risk to the rights and freedoms' of EU citizens but did not pose a 'real risk of significant harm' to Canadian citizens, thus requiring notification under the GDPR but not under Canada's law.[38]

Some jurisdictions do not impose any harm thresholds either for defining a breach or setting forth the circumstances in which notification is required. For example, South Korea's data privacy law applies no harm threshold to the notification requirement.[39] Similarly, California's breach notification law imposes no harm threshold; rather, an organisation must notify affected California residents of any breach where 'unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorised person'.[40] Under these standards, actual or potential harm to individuals is not considered with respect to whether an organisation must notify individuals of a breach.

If the relevant threshold triggering a mandatory notice requirement is not met, then any notification to individuals or regulators by the impacted organisation would be voluntary. Regulators in some jurisdictions encourage such voluntary notification by organisations, even if the breach does not rise to the threshold that would require mandatory notification. Argentina, for example, has no mandatory breach reporting requirements but encourages organisations to have a plan to manage breach incidents and requires that they maintain a record of data breaches that may be given to the regulatory authority upon request.[41]

Considerations regarding the provision of notice

Once an organisation determines that notification is required or prudent, several considerations arise as to the provision of notice itself, most of which can be addressed in advance in a global breach response plan. Again, the variation between different notification regimes is significant and must be carefully considered to ensure an efficient and coordinated approach.

Who provides the notice

Under the multinational data privacy regime, only certain entities are required to provide notification in connection with a data breach. Some statutes, such as HIPAA, the US federal health law, require only that organisations operating within a specific industry sector provide notice of a breach. Other laws, however, require notification more broadly for all organisations that control or process individuals' personal data.

36 Federal Law on the Protection of Personal Data Held by Private Parties 2010, Chapter III, Article 64.

37 GDPR, Articles 33(1), 34(1).

38 Compare PIPEDA, S.C. 2000, Chapter 5, Section 10.1(1) and GDPR, Articles 33(1), 34(1).

39 Personal Information Protection Act, Article 34.

40 Cal. Civ. Code § 1798.82(a)(1), (b).

41 See Recommended Security Measures for the Processing and Conservation of Personal Data, AAIP Resolution No. 47/2018. Notably, Japan currently encourages voluntary notification in the event of a data breach, but a recent amendment to the Japanese Act of the Protection of Personal Information, which will take effect in 2022, will make such notification mandatory.

Several of the comprehensive data protection laws currently in effect require that all controllers of personal data notify individuals and regulators of a data breach. Although controllers of personal data are required to provide notice to individuals and regulators (or face penalties), the controller may not always be the entity that discovers a breach. The processors of data may be more likely to find evidence of a breach as they perform their work with the data, and for that reason a number of notification regimes require processors to notify the controller if they discover a breach. For example, the GDPR requires that the processor notify the controller 'without undue delay' after the processor becomes aware of a breach. Virginia's breach notification law also requires that those entities that maintain data that they do not own or license (i.e., processors) must report a data breach to the owner or licensee of the data (i.e., controllers) 'without unreasonable delay' after discovery of the breach.[42] These notification requirements for processors ensure that controllers will be able to timely meet their own notification obligations.[43]

Timing of notice

Many data privacy statutes require notification quickly after the organisation has discovered the breach and the scope of its impact. California's data breach notification statute, for example, requires that notification be made to individuals 'in the most expedient time possible and without unreasonable delay' following discovery or notice of the breach.[44] Notification may be reasonably delayed under California's statute to allow the organisation time to assess the scope of the breach or to prevent any interference with an ongoing criminal investigation. Several other states, including Virginia, New York and Massachusetts, require notice to data subjects without 'undue' or 'unreasonable' delay.[45] The same standard is seen in data privacy laws in other jurisdictions, such as the EU, which also requires notice to data subjects 'without undue delay'.[46]

The specific requirements vary in some statutes for notification to regulators as opposed to individuals. Some statutes may not require notification to a regulator at all unless a certain number of data subjects have been affected. California's statute, for instance, requires that there be at least 500 affected California residents before requiring that notification be made to the state attorney general. In other jurisdictions, the notice requirement for regulators is not tied to any number of affected individuals. For example, India's data protection law broadly requires organisations to 'report the cybersecurity incidents to [the regulator] within

42 Va. Code Ann. § 18.2-186.6(D).

43 This is an area where contractual considerations often arise. Controllers and processors of data maintain a symbiotic relationship, whereby controllers own and are responsible for data that may be in the possession of processors. This presents particular risks in the event of a data breach that occurs in connection with personal data a third party is processing on behalf of a controller. Controllers and processors frequently allocate these risks by entering into contracts that impose their own notification requirements and determine liability protection and exposure. Typically, controllers will seek to include specific time requirements for notification from the processor (such as within 48 hours of identifying a breach) and assignment of liability to the processor in the event of a data breach that is attributable to the processor's conduct. Processors, by contrast, typically will seek to limit their exposure in the event of a breach that may occur while the processor is in possession of the personal data.

44 Cal. Civ. Code § 1798.82(a).

45 Va. Code Ann. § 18.2-186.6(B); N.Y. Gen. Bus. Law § 899-AA(2); Mass. Gen. Laws, Chapter 93H, § 3.

46 GDPR, Article 34(1).

a reasonable time of occurrence' of the breach.[47] There is also variability in the time period to provide notice to regulators and data subjects. The GDPR, for example, specifies that notification must be made to the national supervisory authority (or lead supervisory authority in the case of cross-border breaches) 'not later than 72 hours after having become aware of' the data breach; if the supervisory authority is not notified within that window, the organisation must provide reasons for the delay.[48] This differs from notification to data subjects under the GDPR, which must be made 'without undue delay' but without reference to a specific time period.

Organisations impacted by a breach thus must assess differing notice timing requirements for regulators and data subjects both within a particular statute and across multiple jurisdictions.

Form and content of notice

Statutory requirements also vary with respect to the form and content of the data breach notice. The GDPR, for example, requires that the notice to the regulatory authority:

- describe the nature of the breach;
- provide the name and contact details of the company's data protection officer;
- describe the likely consequences of the breach; and
- describe the measures taken or proposed to be taken by the controller to address the breach.[49]

Other statutes are even more prescriptive with respect to the required form and content of the notice. California's breach notification statute, for instance, requires that the notice to individuals use a certain title ('Notice of Data Breach') and headings ('What Happened?'; 'What Information Was Involved?'; 'What We Are Doing'; 'What You Can Do'), that the title and headings be clearly and conspicuously displayed, and even that the text of the notice use no smaller than 10-point font.[50] The California statute also provides a model breach notification form that companies may use as a template for their notice, and the use of which ensures compliance with the statutory requirements.[51]

Public messaging

In addition to complying with regulatory requirements in the aftermath of a breach, organisations face the communications challenge of conveying an appropriate public message. Media outlets will quickly discover and report on any large-scale data breach – often triggered by a notification submitted to a data regulator or a public company's securities disclosure

47 Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013, § 12(1)(a).

48 GDPR, Article 33(1).

49 id. Given the difficulty organisations frequently face in describing all of these elements within 72 hours of having become aware of the breach, the European Data Protection Supervisor's Guidelines permit phased reporting. European Data Protection Supervisor, Guidelines on Personal Data Breach Notification for the European Union Institutions and Bodies, Section 5.2 (Nov. 21, 2018).

50 Cal. Civ. Code §§ 1798.82(d)(1)(A-C).

51 id. at § 1798.82(d)(1)(D).

(see above). In turn, an organisation's management and directors frequently face pressure to release public statements to the media addressing the breach and any remedial steps taken. There are many facets of the communications strategy that are beyond the scope of this chapter, but from a regulatory standpoint what is critical is including in an organisation's incident response plan – and then following in the event of a breach – a tight internal coordination mechanism involving the legal and relevant global business functions to enable a measured, consistent approach to all public statements.

Data security compliance and enforcement observations

Separate and apart from the issue of notification, organisations that have experienced a data breach face a range of other potential regulatory challenges. For instance, all organisations must prepare to respond to regulatory inquiries with the potential to lead to an enforcement response, whether tied to an underlying security failure, the adequacy of the notification or some other issue. And public companies have the added challenge of evaluating whether the breach is material to their financial performance or operations and thus may be required to be disclosed to investors. As regulators across the globe gain in enforcement experience and begin to coordinate law enforcement activity with one another, organisations must increasingly be prepared to navigate the added complexities posed by these challenges when they arise in the context of multi-jurisdictional investigations of cross-border data breaches.

Data security

Many data protection laws contain provisions requiring organisations to maintain the security measures necessary to protect individuals' personal information from unauthorised access. For example, the GDPR requires that companies take 'appropriate technical and organisational measures' to ensure that data is securely stored and processed.[52] The California Consumer Privacy Act (CCPA) requires that organisations 'implement and maintain reasonable security procedures and practices' to protect California individuals' personal data.[53] And Mexico's data protection law requires that all data controllers and certain processors 'establish and maintain administrative, physical, and if applicable technical, security measures' to protect personal data.[54] These and other similar laws establish standards that data protection authorities and other enforcement agencies are increasingly using to hold organisations accountable if a data breach occurs that, in the view of regulators, should have been prevented or mitigated.

The GDPR permits regulators to pursue fines for data security violations equal to the higher of €20,000,000 or 4 per cent of an organisation's annual worldwide turnover.[55] In Brazil, the LGPD will permit regulators to pursue half that amount once the administrative sanction provision comes into force in August 2021.[56] California takes a different approach

52 GDPR, Article 5(1)(e).

53 CCPA § 1798.150(a)(1).

54 Federal Law on the Protection of Personal Data Held by Private Parties, Chapter III, Article 57. Mexico's law further identifies factors and actions that data controllers must take into consideration in determining security measures. Id. at Articles 59–61.

55 GDPR, Article 83(5).

56 See Ken Silva, 'LGPD sanctions postponed until August 2021', Global Data Review (12 June 2020), https://globaldatareview.com/coronavirus/lgpd-sanctions-postponed-until-august-2021.

and permits the state attorney general to seek civil penalties (calculated with respect to each affected consumer) of up to US$7,500 per intentional violation and US$2,500 per unintentional violation, with no maximum amount.[57] In the context of cross-border data breaches, the total amount of regulatory fines that could be imposed on an organisation by multiple enforcement authorities – and the potential for duplicative penalties given different approaches to conceptualising the fine amount and different definitions of data subjects and consumers – are both significant.

Public company disclosures

Public companies impacted by a breach face additional regulatory requirements. For instance, in the United States, the Securities and Exchange Commission (SEC) has issued interpretative guidance requiring public companies to disclose material cybersecurity incidents, including data breaches, in their public filings.[58] Even a non-material breach may give rise to a disclosure obligation where investors should be informed of potential risks the company faces. And in the European Union, the Market Abuse Regulation (MAR) requires EU-listed companies to disclose 'inside information', which potentially includes data breaches and other types of cybersecurity incidents, that directly affect their operations and the price of financial instruments.[59] Public companies thus must carefully determine both whether notification and disclosure of data breaches is required, as well as the potential impact one determination may have on the other. As the SEC's 2018 settlement with Yahoo makes clear, the issue of disclosure to investors can lead to significant enforcement consequences.[60]

The future of enforcement

Many data protection authorities around the world are still in the early phases of enforcing data protection laws and managing their budgetary constraints, and organisations will be monitoring enforcement trends closely. For instance, organisations will be watching for signs of the emerging enforcement priorities of Brazil's data protection authority once the LGPD's administrative sanctions go into effect in August 2021, and the impact of the California Privacy Rights Act, the successor to the CCPA that will divide enforcement between the California AG and a newly created data regulator when it goes into effect in January 2023, on the overall US enforcement landscape.

Organisations will also be closely watching for trends toward coordinated resolutions of enforcement actions among data protection authorities from different countries. We

57 CCPA § 1798.155(b).

58 Securities and Exchange Commission, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8166, 8168 (Feb. 26, 2018). This guidance followed earlier guidance issued by the SEC's Division of Corporation Finance in 2011. See Securities and Exchange Commission, CF Disclosure Guidance: Topic #2 (13 October 2011), www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

59 See MAR, Article 17(1); see also 'Untangling the Tangled Web of Cybersecurity Disclosure Requirements: A Practical Guide', Harvard Law School Forum on Corporate Governance (17 June 2018), https://corpgov.law.harvard.edu/2018/06/17/untangling-the-tangled-web-of-cybersecurity-disclosure-requirements-a-practical-guide/.

60 Press Release, 'Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees to Pay $35 Million', Securities and Exchange Commission (24 April 2018), www.sec.gov/news/press-release/2018-71.

have seen such coordination among US federal and state regulators, and within the EU, following cross-border data breaches. But while there have been examples of enforcement actions announced by multiple countries at different times in connection with cross-border data breaches (e.g., *Equifax*, *Yahoo* and *Starwood/Marriott*), it remains to be seen if and when regulators from different countries may begin to announce coordinated resolutions of the type we have come to see in corporate criminal investigations.[61] In the meantime, we anticipate debate about whether the merits of such an approach, such as encouraging cooperation among enforcement agencies and avoiding duplicative penalties for organisations, apply in the data breach context.

Conclusion

Today's complex regulatory environment presents great challenges for global organisations contending with a data breach of any magnitude. Compliance with the multitude of international breach notification laws requires an understanding of what facts may trigger statutorily mandated notice obligations and how and to whom that notice must be communicated. Even when breach notification obligations are satisfied, organisations still must be prepared to handle other regulatory challenges as well, including inquiries into security vulnerabilities that may have contributed to the breach. As more countries enact comprehensive data protection laws and cross-border data breach enforcement picks up, organisations that have breach response procedures that are carefully prepared and reflect a nuanced, global perspective will be best positioned to handle a major incident.

61 See, e.g., 'Airbus to pay $4 billion to settle bribery probes', Global Investigations Review (31 January 2020), https://globalinvestigationsreview.com/airbus-pay-4-billion-settle-bribery-probes ('Airbus has entered into the largest foreign corruption settlement of all time to resolve investigations by authorities in the US, UK and France. Courts in Paris, London and Washington, DC, each approved agreements on 31 January that total €3.6 billion ($3.9 billion) to resolve [the allegations]. The resolutions mark the end of a three-and-a-half-year joint investigation by the UK Serious Fraud Office (SFO) and France's National Financial Prosecutor's Office (PNF), as well as a parallel probe conducted by the US Department of Justice and State Department.').

Appendix 1

About the Authors

Evan Norris
Cravath, Swaine & Moore LLP

Evan Mehran Norris is a partner in Cravath, Swaine & Moore LLP's litigation department and a member of the investigations and regulatory enforcement practice and data security and privacy practice. He focuses on advising US and multinational companies, board members and senior executives with respect to government and internal investigations, criminal defence, regulatory compliance and related civil litigation, with particular emphasis on cross-border, multijurisdictional investigations. Mr Norris has represented clients across numerous industries in a variety of sensitive matters concerning the FCPA, corporate fraud, trade sanctions, cyber incidents, data privacy, anti-money laundering controls and securities fraud. Prior to joining Cravath, Mr Norris served for 10 years as a federal prosecutor in the US Attorney's Office for the Eastern District of New York. He was the lead prosecutor of the groundbreaking *FIFA* case, spearheading a global investigation of corruption in international soccer in one of the most far-reaching cross-border corruption cases ever brought by the DOJ. Mr Norris also served as Chief of the National Security and Cybercrime Section, in which role he was responsible for conducting and supervising matters ranging from ransomware attacks, international data breaches and corporate insider cyberattacks to counterterrorism, counterintelligence and export control cases.

David M Stuart
Cravath, Swaine & Moore LLP

David M Stuart is a partner in Cravath, Swaine & Moore LLP's litigation department. Mr Stuart represents and advises public and private companies, executives and board members in their most sensitive and complex civil, criminal and internal investigations and related securities and derivative litigation. His matters regularly involve allegations of accounting fraud, foreign corruption, insider trading, market manipulation, money laundering, trade sanctions, illicit cyber activity and sexual harassment. He has also conducted comprehensive

reviews of corporate compliance programmes and advised organisations on implementation of best practices in regulatory compliance. He participates in the firm's efforts related to blockchain and financial technology (fintech). From 2000 to 2006, Mr Stuart served in the Division of Enforcement at the Securities and Exchange Commission in Washington, DC. While at the SEC, he supervised a team in the SEC's Financial Fraud Task Force and regularly coordinated multinational investigations with the FBI, the DOJ, and multiple international regulators and law enforcement agencies. For this work, he twice received the Director's Award for outstanding contribution to the enforcement of the federal securities laws. After leaving the SEC, Mr Stuart served as senior counsel of investigations and regulatory affairs for the General Electric Company before returning to Cravath.

Richard J Stark
Cravath, Swaine & Moore LLP

Richard J Stark is a partner in Cravath, Swaine & Moore LLP's litigation department. Mr Stark is recognised as a leading litigator in complex business litigation and has particular expertise in software, computer systems, microelectronics and standard-setting organisations, as well as deep litigation experience in the pharmaceuticals industry. He has a master's degree in Computer Science (machine learning) and is a registered patent attorney. He has represented clients across a range of industries, including technology, life sciences and banking. Spanning nearly three decades, his broad litigation practice and expertise encompasses multifaceted and multijurisdictional business disputes in the realm of intellectual property, antitrust, securities and general commercial litigation, as well as arbitration. Mr Stark's clients have included Qualcomm, Alarm.com, Blue Yonder, IBM, Xerox, Bristol-Myers Squibb, Sanofi-Synthelabo, GlaxoSmithKline, Mylan Laboratories, Illumina and Credit Suisse. In the federal system, Mr Stark is admitted to practise before the US Supreme Court, the Federal Circuit, the DC Circuit, the Second, Third, Seventh and Ninth Circuits, the Southern and Eastern Districts of New York, the Northern, Southern and Central Districts of California, and the District of DC (among others).

Cravath, Swaine & Moore LLP
825 Eighth Avenue
New York, NY 10019
United States
Tel: +1 212 474 1000
dstuart@cravath.com
enorris@cravath.com
rstark@cravath.com
www.cravath.com

Cravath, Swaine & Moore LLP

Data breaches and similar incidents pose a unique challenge – those targeted must both respond and investigate simultaneously. It is an art that is impossible without preparation.

Businesses wishing to prepare will find this volume, *The Guide to Cyber Investigations*, invaluable. It identifies every issue to consider when creating a response template and implementing it, giving both the law and plenty of practical and tactical advice.

Written by leading contributors, all with broad experience of serious data incidents, it is an indispensable desktop guide and a worthy companion to GIR's larger volume on cross-border investigations, *The Practitioner's Guide to Global Investigations*.

Visit globalinvestigationsreview.com
Follow @giralerts on Twitter
Find us on LinkedIn

an LBR business

ISBN 978-1-83862-595-5