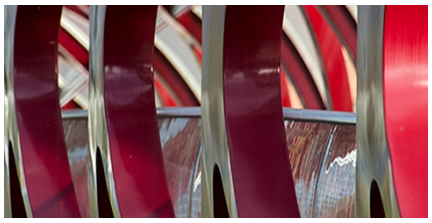
masuda funai



News & Types: 商事／競争／取引関連情報

米国におけるデータ侵害通知義務に関する法律の概要

10/8/2020

By: ケントン クノップ

Practices: 商事／競争／取引, 知的財産テクノロジー

概要

近年、TargetやHome Depotなどの小売業者が保存する顧客のデータが広範囲にわたって漏洩され、その後に被害を受けた顧客がクラスアクションを提起したというニュースを頻繁に耳にするようになり、米国で手厚いデータ保護法の制定を求める機運が高まっています。EU一般データ保護規則(European Union's General Data Protection Regulation(GDPR))のような統一データ保護法のある法域とは異なり、米国には、包括的な連邦データ保護法がありません。代わりに、州法と連邦法のパッチワーク（寄せ集め）が現在の米国データ保護法を形成しています。現在に至るまで、米国のデータ保護法は、各州のウェブサイト・プライバシーポリシー法（カリフォルニア州オンライン・プライバシー保護法(California Online Privacy Protection Act (CalOPPA)など)、各州の一般プライバシー法（カリフォルニア州消費者プライバシー法(California Consumer Privacy Act(CCPA))、ワシントン州の新プライバシー法、イリノイ州バイオメトリック情報プライバシー法(Illinois Biometric Information Privacy Act)など)、各州データ侵害通知法および特定の種類の情報の保護を定める連邦法[1]を含むいくつかの異なる形を取ってきました。このようにデータ保護に関して異なるアプローチが取られている中でも、データ侵害通知法の導入割合は特に高いものとなり、2020年現在、全50州、コロンビア特別区、グアム、プエルトリコおよびバージン諸島でデータ侵害通知法案が可決されています。[2] データ侵害通知法の目的は、個人に関する特定のデータを取得するエンティティに、漏洩の対象となった個人に対して適時に漏洩／侵害の通知を行う作為義務(affirmative obligations)を課し、場合によっては、州当局への通知も義務づけることです。本稿を通じて、これらのデータ侵害通知法に関する認識を高め、その中でも特に注目すべき点を知っていただけることを願っています。

どのようなデータが対象となるのか？

データ侵害通知法は、個人の「個人情報(personal information)」または「個人識別可能情報(personally identifiable information)」について定めています。個人識別可能情報は一般的に、個人のファーストネームもしくはイニシャルおよびラストネームと、暗号化されていないセンシティブデータ（例えば社会保障番号(social security number)、運転免許証番号、銀行口座番号、クレジット／デビットカード番号、医療健康保険情報またはコンピュータ・ユーザー名とパスワードなど）の組み合わせと定義されます。適用範囲は狭いもの

の、いくつかの州においてみられる個人識別可能情報の定義からの除外規定として、一般に連邦、州または地方自治体政府の記録から合法的に入手できる情報が挙げられます。

どのようなエンティティがデータ侵害通知法の適用対象となるのか？

一般的に、データ侵害通知法は、個人識別可能情報を含むコンピュータ化されたデータを所有し、またはこれについて使用許諾を受ける個人や事業体に適用されます。さらに、コンピュータ化されたデータの所有者や被使用許諾者（ライセンシー）に代わってコンピュータ化されたデータを保持するサービスプロバイダーにも、一般的にデータ侵害通知法が適用され、サービスプロバイダーが漏洩にみまわれた場合には、データ所有者に通知しなければなりません。

漏洩／侵害とは何か？

一般的に、「漏洩（侵害）」とは、コンピュータ化されたデータが権限を有しない者により取得され、それにより個人または事業体が保持する個人識別可能情報の安全性、機密性または完全性が脅かされることと定義づけられます。漏洩は、ハッキングによる事業体のコンピュータ・システムへの無断アクセスなどのデジタルな手段、または個人識別可能情報を含んだ会社の所有物の窃盗などのフィジカルな手段によって生じ得ます。さらに、多くの州において漏洩が認識された場合の「危害のリスク(risk of harm)」分析について定められており、この場合には、危害リスクの認識度が特定基準に達する場合に漏洩に関する通知義務が課されることになります。

侵害通知は誰に送るべきか？

各州のデータ侵害通知法は、当該州の住民を保護する機能を有します。各州のデータ侵害通知法のもとでは、ある州の住民は、当該州の法に従った侵害通知を受け取る必要があります。したがって、全50州、コロンビア特別区およびアメリカ合衆国の海外領土の住民に影響を及ぼすようなデータ漏洩が生じた場合は、各法域の固有の要件を充足する、50以上の異なるバージョンの通知が必要となる可能性があります。

さらに、いくつかの州では、一定人数（一般的には500人以上）の州民に影響を与えるような漏洩が生じた場合には、州の司法長官や他の州当局に対する通知が義務づけられています。もっとも、州当局への通知義務を定める州であって、通知を義務づける最低基準値となる住民の数を定めていない州もあります。そのような州では、漏洩の被害に遭った住民がひとりしかいない場合でも、州当局に通知する義務があるということになります。

いつ通知しなければならないか？

通知のタイミングについては、州ごとに大幅に異なることがあるため、各州で適用される法律を精査する必要があります。通知は、漏洩が生じたことを発見してから、または漏洩があったことの通知を受けてから「可能な限り速やかに、かつ不当な遅滞なく」しなければならないというのが最も一般的な規定です。しかし、いくつかの州では漏洩が発見されてから特定の期間内に通知することを厳格に義務づけており、その場合の通知期間は最短30日（コロラド州、フロリダ州、ワシントン州）から最長90日（コネチカット州）、最も一般的に

は45日です。また、多くの州では、捜査機関による捜査およびデータシステムの完全性の修復に時間を要することによる通知の遅れを許容しています。

どのように通知しなければならないか？

米国全50州、コロンビア特別区、グアム、プエルトリコおよび米国バージン諸島の法律により、書簡で通知することが許されています。電話や電子メールなどの追加的手段による通知が可能か否かは、州によって異なります。さらに、事業体が、通知に要する経費が特定金額（イリノイ州では250,000ドル）を超えること、漏洩の影響を受ける人の数が特定数（イリノイ州では500,000人）を超えることまたは漏洩の通知先の情報を十分に持っていないことを証明できる場合に「代替通知」の実施を許可している州もあります。イリノイ州では、代替通知にあたり、影響を受ける人への電子メールによる通知、最低30日間の事業体のウェブサイトにおける顕著な表示の掲載および州内の主要メディアへの通知を義務づけています。

通知にはどのような内容を記載するか？

通知に含むべき内容も州によって異なります。イリノイ州では、通知には、最低限の情報として、３つの大手消費者報告機関(consumer reporting agencies) (Equifax, Experian, TransUnion)および連邦取引委員会(Federal Trade Commission)の連絡先情報、ならびに個人がこれらの機関から詐欺警報(fraud alerts)とクレジットレポートの凍結を実現するための情報を得ることができることに関する説明を含めることを義務づけています。カリフォルニア州などの他州では、通知の形式および内容に関してさらに詳細な要件が定められています。さらに、カリフォルニア州では、漏洩の影響を受けた個人に最低12ヵ月間無料でクレジット・モニタリング・サービスを提供することを事業体に義務づけており、コネチカット州も、最近、州法を修正し、漏洩の影響を受けた個人に最低2年間無料でクレジット・モニタリング・サービスを提供することを事業体に義務づけました。

侵害通知法を遵守しなかった場合の罰則は何か？

各州は、各州のデータ侵害通知それ自体か、他の関連する消費者保護法のいずれかを通じてエンフォースメントを行います。いくつかの州では、適用されるデータ侵害通知法への違反が不当または詐欺的な取引行為とみなされ、州司法長官その他の政府機関による法執行の対象となったり、事業体に対する民事罰の基礎となります。カリフォルニア州などいくつかの州では、漏洩（侵害）の被害者が事業体を直接訴えることができる私的訴権(private right of action)を認めています。たとえば、データ漏洩により個人識別可能情報が開示されたカリフォルニア州の住民は、カリフォルニア州消費者プライバシー法(CCPA)に基づき、1件の漏洩について住民1人当たり750ドルの法定損害または実際の損害のどちらか高い金額の賠償を請求することができ、また、これらの住民はそれぞれの請求を併合してクラスアクションを提起することもできます。イリノイ州も、州司法長官による法執行およびイリノイ州住民の私的訴権の双方について定めています。

まとめ

本稿執筆時点において、米国議会が再び新たな連邦データ・プライバシー法の導入を検討する可能性を示す一定の兆候があるようにも見受けられます。現状では、事業体も実務家も、データ漏洩が生じた場合は、現在の

連邦法と州法のパッチワークに対処する必要があります。各州のデータ侵害通知法の違いから、データ漏洩対応の複雑さと困難さは増していることからすると、最も重要なのは、漏洩が発見されたときに、適用法に準拠していかに迅速な措置を取ることができるかということです。事業体は、侵害通知を速やかに送ることができるよう、漏洩により開示された情報と漏洩の対象者を迅速に識別することで、顧客や従業員が詐欺的取引や個人情報の盗用の被害を受けるリスクを抑制・軽減するとともに、自らが漏洩の影響を受けた顧客や従業員から訴訟を提起されるリスクを軽減することができます。データ漏洩がいつでも、どのような事業体にも起こりうる今日のデジタル世界では、すべての事業体が、データ漏洩への対処についての計画を準備した上で、従業員に対し、データ漏洩が起きた場合にこれを識別し報告することができるようトレーニングを提供する必要があります。これらの措置を講じることにより、事業体は、法に従い、顧客と従業員の個人データを保護するために最善策をとっているという自信を持つことができます。

---

[1] データのプライバシーと保護に関する連邦法の例： HIPAA (Health Insurance Portability and Accountability Act)個人の医療および他の健康関連情報を保護する医療保険の携行性と責任に関する法律；GLBA (Gramm-Leach-Bliley Act)金融機関に顧客の個人情報と財務情報の保護を義務づけるグラム・リーチ・ブライリー法；およびCOPPA (Children's Online Privacy Protection Act)13歳未満の児童の個人情報を保護する児童オンライン・プライバシー保護法

[2]本稿の目的においては、別途記載がない限り、米国50州、コロンビア特別区、グアム、プエルトリコおよび米国バージン諸島をまとめて「州(states)」と呼ぶ。