TransReflections

Cyber Newsletter

February 2020

TransRe

We value cyber risk.

Table of Contents

Introduction by Elizabeth Geary	02
Notable Breaches	03
Regulatory & Legislative Update	04
Global Cyber Security	06
Litigation News	07
Crypto Corner	08
Cyber Publications	08
TransRe Speaks!	08
How Long Is Your Shadow?	09
Navigating the California Consumer Privacy Act	10

Introduction

Attrition – Good Publicity, But….

Cyber insurance got something of a bad rap in 2019. Multiple media outlets ran stories with a common theme - that cyber policies don't pay. Often the story was based on a misunderstanding, such as the property policy that denied cyber coverage. Although the policy specifically covered data, it also had a war exclusion and that was invoked. All the feverish activity on LinkedIn could not dispel the notion that the cyber promise to pay was somehow hollow.

That's not true. Cyber policies do pay. Until now the cyber market has 'enjoyed' low attritional loss ratios with some scattered (expected) single-risk large losses. However, that is changing rapidly, and losses are quickly emerging.

The major driver of first party losses has been targeted ransomware and the business interruption that follows. Even when a ransom is paid, adjustment costs and business interruption add up quickly. While the ransom "tail" is just a few hours, the other costs may take many months to resolve.
We also see losses from breaches of third party privacy, driven in part by the Biometric Information Privacy Act (BIPA) of Illinois. The act has been in place for more than 10 years, but claims are now finding their way to cyber policies, with additional exposure through other professional lines policies. California's Consumer Privacy Act (effective January 1, 2020) has already resulted in claims against Salesforce and Hanna Andersson. More may be expected.

Increased attritional losses reduce the premium reserved for systemic events. Greater payouts may help stem the bad publicity, but coverages may retract, more controls will be needed and rates will probably have to rise. As prices rise to match loss trend, there will be a greater emphasis on risk management and preventative measures. Risk management is expensive. Large companies have larger budgets, but millions of small companies do not have those resources. To date, cyber profitability has reduced our demand for such risk management practices to be in place, but that will change. Constant monitoring of exposures, and frequent communication with customers will become widespread.

We look for the greater premium pool to support greater insight and greater resilience for the wider business community. The recent Federal decision in Maryland (that a (silent cyber) property policy must pay for damage to data as it was 'physical' damage) should cause more insurers to underwrite, price and write cyber exposures on a standalone basis.

Losses are an important part of product development. As the market notes these loss signals, evaluates coverage, and adjusts its risk management practices, a better, more effective cyber market will emerge.

TransRe's Appetite

Brokers and clients sometimes ask why we focus predominantly on large risk business. Every underwriter has a different perspective, and our view is driven by two considerations: that large risks tend to be better protected, with better IT infrastructure and support and (since it is hard to diversify cyber) we deploy our capacity where we think the best risk reward return lie.

We also have systemic SME concerns. In August 2017, Hurricane Harvey hammered Texas with unprecedented rainfall. Loss adjusters flocked to Texas to help. A few weeks later, Hurricane Irma hit Florida, and some Florida insurer loss adjustment expenses rose from ~7% to ~30%.

Think about the specialist nature of cyber claim adjustment and remediation services. Specific skills are required to assess the damage and/or rebuild the data. Adjustment costs could increase significantly in a systemic attack, as resources focus on the larger risks / limits. Are we underestimating (and undercharging) SMEs for this LAE risk?

And Finally

This is my last contribution to our cyber newsletter. As I pass the baton to Rhett Hewitt, our new global head of cyber, I want to thank of all our team: underwriters, actuaries and especially our claims team for all their support, both in putting this newsletter together, and every day in their diligent efforts to improve our understanding of the ever-evolving cyber space. I look forward to reading Rhett's reflections going forward.

Elizabeth Geary

Notable Breaches

Travelex Ransomware Attack

London-based foreign exchange company Travelex suffered a ransomware attack that forced it to shut its computer systems in 30 countries and then resort to manual processes. The attackers (thought to be a group known as REvil/Sodinokibi) claimed to have downloaded 5GB of sensitive customer data and demanded $6 million. Travelex has reported they have no evidence that any data left the organization.

Major German Manufacturer Targeted by Ransomware

In October 2019, Pilz, a German automation technology company was forced to shut down its networks and servers in an effort to limit the impact of a ransomware attack. Server and communication systems were affected worldwide. The company confirmed that no customer or supplier data had been stolen and no viral proliferation of the attack had been identified.

UK Government Department in New Year Honours Publication Error

The UK government's Cabinet Office has apologized following the release of addresses online of more than a thousand recipients of the New Year Honours list. The New Year Honours list recognizes the achievements of people across the UK and the list included celebrities, senior police officers and politicians. The matter was reported to the ICO.

Jet2: IT Worker Holding a Grudge Jailed

A former IT contractor was jailed for 10 months following an attempted malicious attack against British low-cost airline Jet2. The attacker retained logins to access and delete all user accounts including those with administrative privileges. The airline managed to prevent an attack which would have caused significant disruption.

Sensitive Information Stolen in Mitsubishi Electric Breach

Information on government agencies and business partners, together with the personal data of 8,000 people (including employees) has been stolen in a cyberattack against Mitsubishi Electric. There is speculation that state sponsors are behind the attack on the Japanese electronics manufacturer that took place in June of last year.

Mexico's Pemex Faces $5M Ransomware Demand

Pemex, the Mexican state-run oil company suffered a ransomware attack in late 2019, allegedly of the DoppelPaymer strain. Pemex did not pay the ransom and later reported the company faced up to $71M in cleanup costs with only $3.6M in insurance recoveries.

Two Canadian Banks Subject to Ransomware Attack

BMO and CIBC suffered near-simultaneous ransomware attacks. The ransom demand in each case was $1M in cryptocurrency. The attackers threatened to release customer data if the ransom was not paid.

Municipalities Remain Targets: NOLA and Pensacola

New Orleans declared a state of emergency after hackers infiltrated the city systems, many of which remained down for weeks after the attack. NOLA has disclosed the breach has cost at least $1.5M to date and that they have a $3M cyber insurance policy in place. It's not clear what specific coverages or sublimits (if any) apply within that policy. Elsewhere, Pensacola, FL, was subjected to a ransomware attack demanding $1M. It's believed that the city did not have cyber insurance and did not pay the ransom. Since the attack, the city's new risk manager was tasked with implementing a cyber policy.

Regulatory & Legislative Update

European Regulators Continue to Flex Muscles on Data Protection Breaches

The Berlin Commissioner for Data Protection and Freedom of Information issued a €14.5M fine to a real estate company for violations under GDPR. The company used an archive system to store the personal data of tenants. Any data no longer required should be removed. Data included salary statements, self-disclosure forms, extracts from employment and training contracts, tax, social security, health insurance data and bank statements. During an initial inspection in 2017, the commissioner recommended a change to the archive system. In 2019, the company was unable to demonstrate it had cleaned up the database in a follow up inspection.

Also in Germany, the Federal Commissioner for Data Protection and Freedom of Information (BfDI) imposed a €9.6M fine on telecommunications service provider 1&1 Telecom GmbH. The company did not establish sufficient technical and organizational measures to prevent unauthorized persons from being able to obtain customer information via the customer hotline service.

The UK's ICO issued the maximum fine possible (£500,000) under the old Data Protection Act following systematic failures in the way DSG Retail Limited safeguarded personal data. An attacker installed malware on over 5,000 cash registers at DSG stores and collected personal data over a period of nine months. Details of 5.6M payment cards were accessed along with the personal information of approximately 14M people. Carphone Warehouse, part of the same group, was fined £400,000 by the ICO in January 2018 for similar security vulnerabilities. The ICO observed that contraventions would have been much higher under GDPR.

French regulator, CNIL issued a €500,000 fine against a company that specializes in thermal insulation of private homes. Futura Internationale failed to effectively implement client opt-out requests, and failed to provide enough safeguards to enable international transfers of data to call centers located outside the EU.

Companies Settle FTC Claims Over Privacy Shield Participation

Five companies, accused of allegedly misrepresenting that they were certified under the EU-US Privacy Shield framework, have settled with the US Federal Trade Commission (FTC). Privacy Shield allows personal data to be transferred between the US and EU in compliance with data protection laws.

In October of last year, the EU Commission confirmed its adequacy decision in relation to Privacy Shield, the legal framework for data transfer between the EU and the US. Various concrete steps need to be taken to ensure better compliance with Privacy Shield in practice.

Facebook Pays Record $550M BIPA Settlement

In the largest settlement of alleged violations of Illinois' Biometric Privacy law to date, Facebook has agreed to pay $550M to resolve a class action lawsuit. Class members include essentially all Facebook users who are residents of Illinois. The lawsuit was based on Facebook's automatic photo-tagging software that reviews all photos uploaded to the site and uses facial recognition technology (a tech that falls under BIPA) to match people in the photos to Facebook users without the appropriate disclosures.

Right to Be Forgotten

The German Constitutional Court ruled that a man convicted of murder 37 years ago has the right to have his name removed from online search results. The case was originally rejected in 2012 on the basis that his rights did not outweigh the public interest.

Separately, this past September, the CJEU affirmed that the right to be forgotten is not global. If a search engine operator grants a request to be de-referenced, the operator is not required to carry out that de-referencing on all versions of its search engine and is only required to remove links on versions in member states

India's Revised Data Protection

India's government has introduced a Data Protection Bill recognizing the fundamental right of privacy. The bill, which will be subject to the scrutiny of a joint parliamentary committee, develops a comprehensive data governance framework. The Data Protection Bill has incited some criticism from business communities for overreach beyond privacy issues.

Mandatory cyber security for power grids has also been included in draft rules published by the Central Electricity Regulatory Commission of India. The draft proposals include the requirement for operators to install firewalls and other measures to reduce the risk of cyberattacks.

US Senators Urge Investigation into Amazon's Role in Capital One Breach

Following the breach of over 100M Capital One records in July 2019, two US senators have urged the FTC to investigate Amazon and the company's role in the breach - Amazon Web Services hosted the servers at issue.

Bill Introduced to Create US Federal Privacy Agency

With no current federal privacy regulation, the Online Privacy Act has been introduced to Congress. It would create a new federal agency (dubbed the Digital Privacy Agency) to provide uniform oversight of the personal data collected by numerous companies. The prospects for the legislation are currently unknown.

New York State Legislature Considers Ban on Ransomware Payments

As discussed elsewhere in this newsletter and in previous editions, US municipalities remain frequent targets of ransomware attacks. There has been some discussion between state governors not to pay such ransoms (since they bankroll the next attack). Now the New York State legislature is considering a bill to prevent state and local governments using taxpayer funds to pay ransoms, on the theory that doing so removes the incentive of ransomware operators to target New York. The bill would simultaneously create a "Cyber Security Enhancement Fund" for use by municipalities of less than 1M residents to upgrade their cyber security measures. Notably, the bill would not prevent municipalities from purchasing cyber insurance, when their insurer would make any ransom payment rather than the municipality.

Biometric Privacy: The Next Frontier?

The Illinois Biometric Privacy Act (BIPA) has made headlines as the first law that creates a private right of action (allows individual citizens to sue rather than just the Attorney General). This may not always be the case: However, New York, Florida and New York City have proposed similar laws that are under review and that would each create a private right of action.

Cayman Islands Data Protection Law Takes Effect

The Cayman Islands has put into effect its own Data Protection Law (DPL) which closely mirrors the European GDPR.

Global Cyber Security

Russian Hacking Group Poses as Iranian Hacking Group

A Russian hacking group variously known as Turla/Waterbug/Venomous Bear recently claimed it had hacked an Iranian hacking group and stolen its cyber tools to hack a wide range of companies and government offices. The hacking mission appears to obtain sensitive documents and transfer blame to the Iranian government for future attacks.

"Ransomware Superhero" Provides Decryption Keys for Free

Michael Gillespie has been credited with helping hundreds of ransomware victims decrypt their files for free. He has been cracking the encryption codes himself and posting the decryption tools online. Mr. Gillespie and others like him estimate that of the roughly 800 basic ransomware programs, there are over 100 free decryption tools available.

Australian Regulators Sue Google

The Australian Competition and Consumer Commission (ACCC) sued Google in late 2019, alleging the company misled Australians on issues related to how personal location data was being tracked and collected. The allegations claim that the process to turn off location-tracking is misleading and difficult, and that people are left with the impression that location tracking is turned off before it is actually disabled.

Lloyd's and University of Cambridge: Asia-Pac Port Attack Could Cost US $110B

In a recent report it was shown that a single cyber attack across multiple Asia-Pac ports could set in motion a total loss of over US $110B, including over US $100B in uninsured losses. The report illustrates the complexity and interconnectivity of the global economy. The report was co-sponsored by TransRe and is available here.

Project Nightingale: Google and Ascension Investigated for Sharing Healthcare Data

Google faces another investigation; this time for potentially violating the US patient privacy law, HIPAA. In a joint venture with Ascension healthcare group, Google is collecting and analyzing the healthcare data of "tens of millions" of patients. Although Ascension leadership asserts the project is HIPAA-compliant, Ascension employees were the ones who raised concerns about the program. The program is reminiscent of a similar project DeepMind, where London's Royal Free Hospital shared data with Google. This program was found unlawful at the time.

Amazon / Ring Under Fire for Lack of Security

Five US senators have made inquiries with Amazon-owned Ring security cameras over evidence that a number of individuals in Ring's Ukrainian office had full access to security cameras worldwide. According to one report, an individual's email address is the only piece of information needed for employees to look up video feeds. In other news, an investigative report found that software that easily breaks through Rings' security is available for purchase on the dark web.

Antivirus Program Avast is Harvesting and Selling User Data

Avast Antivirus is one of the largest antivirus vendors in the market. In January, the company was found to be using a subsidiary company to sell browsing history data harvested from Avast users. The subsidiary (called Jumpshot) sold this data to a number of companies, including Google, Yelp, Microsoft and others. The data is sold for millions of dollars and includes an "All Clicks Feed" that allegedly tracks user behavior, clicks and movement within websites in granular detail, including what searches they made within a site and what videos they watched.

Healthcare Industry Remains Prime Target for Hackers

The combination of sensitive data and tight budgets often prevent meaningful cybersecurity. With massive amounts of data, the healthcare industry is among the most-targeted for cyber breaches. One report pegs 2019 losses in the healthcare industry alone at over $4B, with the outlook for 2020 being worse. The report lists a few statistics showing that the healthcare industry isn't prepared to face the cyber challenges in today's world.

"Anonymized" Data a Misnomer?

A cornerstone of the data sales industry is the assertion that consumer data, once "anonymized" can safely be sold without risk to the consumer and crucially without application of strict regulation. In 2015, a UK study correctly identified 99.98% of individuals from anonymized data. Another study from MIT correctly identified 90% of users using just four vague data points. More recently, two Harvard students completed the task for a class project using data from multiple leaks available on the dark web, "they form a surprisingly clear picture of our identities."

Litigation News

Storing Cookies Requires Internet Users' Active Consent

The Court of Justice for the European Union (CJEU) has ruled that Internet users must give consent to a website in regards to the access of cookies on equipment by deselecting pre-checked boxes.

Morrisons Case Before UK Supreme Court

In November 2019, the UK's Supreme Court heard the appeal in the Morrisons vicarious liability case. The court will determine whether the supermarket chain is liable for the criminal acts of an employee who leaked personal details of thousands of employees online. The court's ruling is still pending.

Biometric Privacy Act Claims May Face Challenge in Federal Courts

The Illinois Biometric Privacy Act (BIPA) has been a popular topic in the last year. The Illinois State Court ruled that a technical violation of the statute was sufficient to meet "standing" requirements, and hundreds of lawsuits followed the ruling. However, in a recent case that was moved to federal court, the US District Court for the Northern District of Illinois repeatedly belittled the idea that such a technical violation (in this case the failure to provide written notice of the collection and storage of fingerprints used to clock employees in and out) could ever be sufficient to grant standing. The court found this to be the case where the employee-Plaintiff knew their fingerprints were taken and that they were being stored, making the requirement for written notice redundant.

Healthcare System Sues Third-Party Service Provider for NotPetya

Pennsylvania-based Heritage Valley Health System has sued Nuance Communications after there was a breach by NotPetya in 2017. The attack shut down Heritage Valley Health System's medical equipment which prevented physicians from accessing patient records.

Cyber Latest Avenue for D&O Lawsuits

Many recent large breaches have resulted in a lawsuit against the Board of the breached entity, raising the question what are the duties of every board member in light of modern cyber risks?

Court Finds Coverage for Business Email Compromise

US Federal District Court in New York has found coverage under AIG's "Risk Protector" policy for a $6.9M business email compromise loss. Notably, the policy is not a standalone cyber policy, it is an E&O policy.

US Court Holds Loss of Data Covered by Property Policy

Federal District Court in Maryland ruled in January 2020 that damage to intangible data in a ransomware attack constituted "direct physical loss or damage" under the insured's property policy, and therefore found coverage to be in place. In this case, coverage included replacement of the entire computer system. This arguably unintended coverage for cyber loss under a property policy is a good reminder that significant Silent Cyber exposure remains unrecognized in the insurance world.

Crypto Corner

- The U.S. Securities and Exchange Commission (SEC) has become increasingly aggressive in their regulation and enforcement of cryptocurrency-related issues, which is in line with a more-active SEC as well.
- The English High Court has granted an interim injunction against a crypto exchange, to an insurer seeking to ultimately recover bitcoin paid to cyber-extortionists in a ransomware attack. Cryptocurrency has long been the preferred payment method for cybercriminals. This case demonstrates that with quick action, legal remedies may be possible.

Blockchain Reinsurance Platform Launches

The Blockchain Insurance Industry Initiative known as B3i launched a blockchain-based trading platform in late 2019 for the property-catastrophe XOL marketplace. B3i is backed by 19 global (re)insurance companies. This project is intended as a proof-of-concept to cut administrative costs in the reinsurance marketplace.

Cyber Publications

NetDiligence 2019 Cyber Claims Study

Vince Vitkowsky of Gfeller Laurie: Cyber Risks and Insurance Coverage Decisions 2015-2019

TransRe Speaks!

February 6th **Peter Cridland** will appear on a panel sponsored by the Queens Chamber of Commerce, to discuss new Cyber Laws and the impact they'll have on a small business

March 19th- 20th **Peter Cridland** will join a panel to discuss cyber coverage at the International Bar Association: Insurance Without Borders conference in London

April 28th **Rhett Hewitt** will speak at the Trans Re Europe Liability Discussion Forum in Munich

How Long is Your Shadow?

By: **Neil Inskip**, TransRe London's IT Manager

Owing to some severe editorial intervention, I am unable to start with an amusing anecdote that involves black magic and chalk hexagrams in my server room, and how that causes me sleepless nights. Instead, I must get to the point about "Shadow IT" [about time- Ed.].

Shadow IT is the cause of many sleepless nights in our business. In the past, the IT department was responsible for handling all applications and bundling all IT services for all corporate users. Today, many users serve themselves and shadow IT is the term for any hardware or software not provisioned, governed, supported or sanctioned by the IT department.

This has happened because of the spread of consumer widgets and cloud technology and the productivity gains they offer. Many users adopt the new technology early because the IT department (burdened with risk and compliance requirements) is not able to roll out these agile solutions as quickly as they want. As a result, the juxtaposition between business agility and cyber security is causing major concern.

For example, if you use shadow cloud storage, how do you know the cloud provider is reputable and compliant with GDPR, HPPA, PCI, etc.? Failure to achieve compliance can result in heavy fines. There are practical issues as well - is that newly created cloud data silo backed up? Can you afford to lose the data if it isn't? If you save corporate data to an unapproved cloud data storage (think of any you use) what happens if WannaCry (or any other ransomware) hits it? Compare that to your IT department's approach – they have been protecting your corporate data with hourly backup recovery snap shots, 24/7 monitoring, additional security layers, etc.

If you are doing something business critical on the shadow IT system, what happens when that solution is down? How many cloud-based CRM solutions can offer and deliver those platinum plated "5 9's" (99.999% availability/uptime) to their customers?

For many organizations, the use of shadow IT within their organization has snuck up on them without their knowledge or approval. The question now is how to remedy the situation, which involves a two step process:

First, stem the flow (nip it in the bud) and issue a policy for the required behavior (to eliminate the free-for-all) and to acknowledge that all corporate technology must be fully understood and approved before it is deployed.

Second: identify how deep the issue goes. You can survey your staff to identify what "shadow tech" is being used, but the intelligent approach involves discovery software to examine your firewall traffic, desktop PCs and servers. That inventory is matched against users to capture all technology in use. Software audit packages (usually already in place for software licensing proposes) are a very good place to start. From there you prioritize the risks and work down the list to eliminate them. If something is totally unacceptable, block its use and replace with an approved solution (which is hopefully better anyway).

A presenter at Microsoft's 2018 Ignite conference said that 80% of workers use non-sanctioned cloud applications. Of those applications, 61% were used without the knowledge of the IT department. Playing catch-up has become the new norm (although I should also mention that many companies have had no problems with shadow IT behavior).

So, the next time you want to know whether you can still buy chalk, and you want to ask Alexa to put it on your shopping list, please wait till you get home. Alexa is not yet an approved co-worker at TransRe.

Navigating the California Consumer Privacy Act

Guest Column by: **David Artman, Christopher Ballod** and **Alyssa Watzman** of Lewis Brisbois Bisgaard & Smith LLP

The California Consumer Privacy Act of 2018 (the "CCPA"), which took effect January 1, 2020, is the most sweeping piece of privacy legislation in the United States to date. It imposes European-style obligations on companies that collect personal information (or have personal information collected for them) and grants new rights to California consumers. As part of the CCPA, the California legislature delegated broad authority to the state attorney general to draft regulations, expand on existing obligations and clarify how companies can implement some of the changes.

An initial draft of the regulations was published in October 2019, and the final version is expected to be published in the Spring of 2020. As determined by the language of the draft regulations, the attorney general fully embraced its broad authority. This article will provide a high-level overview of the four main topics addressed in the draft regulations – (1) requirements for consumer notification, (2) requirements for responding to consumer requests, (3) efforts to verify that consumer requests are valid and (4) special rules for minors. It will also highlight changes that may require businesses to review and revise practices and train employees to be CCPA compliant.

a) Consumer Notices

The regulations provide some clarity with respect to the four types of notice that must be provided to consumers under the CCPA: notice of collection of personal information, notice of the right to opt-out of the sale of personal information, notice of financial incentives and privacy policies. All notices must be written in plain language and must be available in all languages in which the business provides contracts and information to its customers in the ordinary course of business. All notices must be accessible to people with disabilities, use a format that draws a consumer's attention and, if online, be readable on smaller screens (read: cellphones).

Privacy policies must be comprehensive and conspicuous. They must explain certain rights afforded to consumers under the CCPA (right to know about information collected and disclosed, right to request that their information be deleted, right to opt-out of sales of personal information, and right not to be discriminated against) and provide details about what information is collected by the business, and whether the business sells consumer data. They also must provide information about how consumers can submit requests, act through an agent, and how the company verifies consumer requests. In addition, for companies that collect personal information for 4,000,000 or more consumers annually, the privacy policy must disclose detailed metrics about the number consumer requests and the company's response time, among other things.

As to the notice of collection, no business may collect information from a consumer before the notice is posted in a manner consistent with the statute and regulations. The notice must list the specific categories of information collected, how the information will be used, and describe the means by which a consumer can opt-out of the sale of their personal information. A business may not use a consumer's personal information for any purpose other than the purpose listed in the notice of collection. A company that collects information online may use the privacy policy as its notice of collection, provided that the policy contains a link to a section that explains specific information required for the notice.

The notice of a right to opt-out must be posted on the company's Internet page, if it has one. The company must provide a link specifically titled "Do Not Sell My Personal Information" or "Do Not Sell My Info." In addition, the attorney general will provide an icon that companies can substitute in lieu of the language above.

Businesses should keep in mind that the CCPA and its associated regulations apply to both online and offline collection and use of personal information. Companies will need to closely review the requirements of the regulations pertaining to notices, particularly the privacy policy and notice of collection, and re-write their existing policies and notices accordingly.

b) Consumer Requests

The CCPA permits consumers to know what categories of information, and specific data, a business collects about them, and provides the right to request that their information be deleted. The recipient business is obligated to delete from its records and instruct any third parties to do the same, under certain circumstances. Recipient business do not have to delete information if it is necessary to complete the transaction for which it was collected; to provide the good or service requested by consumer; to protect business property; to comply with California Electronic Communications Privacy Act; or to otherwise comply with the law.

The regulations clarify that businesses must provide consumers at least two methods for submitting requests to know and requests to delete. However, the methods for these two categories of requests may differ. For requests to know, the method must include at least a toll-free telephone number and an interactive web-form if the company maintains a website. In addition, the company may provide a designated email address and mail-in form. There is no compulsory method by which a company must allow consumers to submit requests. However, whatever means by which the requests are made, at least one must reflect the primary manner by which the business communicates with consumers. The upshot is that companies that primarily interact with consumers in person may be required to provide three methods of receiving consumer requests.

The deadlines to process the requests are tight. Within ten days of receiving a request for information or deletion, a business must acknowledge the request in writing. It then has 45 days from the date the request was received to either delete the information or provide the information requested. This period includes any time required to verify the request. However, a business can delay an additional 45 days (total of 90 days) if they timely respond to the consumer and explain why more than 45 days are required to respond.

Companies should note that certain categories of information may never be disclosed, despite a consumer's request. These categories include, among others, Social Security numbers, driver's license numbers, medical information and financial account information.

c) Verification

Before a company may respond to a request, it must verify that the requestor is who they claim. The method of verification should be reasonable in light of the sensitivity of the information at issue. If a company maintains online, password-protected accounts for consumers, the business may use the account to verify the individual's identity. However, re-authentication is required before disclosing or deleting any of the consumer's data.

For companies that do not have online customer accounts, the regulations provide variable standards of certainty by which the company must verify the individual's identity. If a consumer submits a request to know categories of information, the business must verify the individual's identity to a "reasonable degree of certainty" by, for example, matching two pieces of data provided by the consumer to data in the business's file. However, where a consumer requests to know specific pieces of information, the business must verify the individual's identity to a "reasonably high degree of certainty" by, for example, matching at least three pieces of personal information, along with receipt of a signed declaration under penalty of perjury stating that the requestor is who they claim to be. Requests to delete must be verified with a reasonable degree or a reasonably high degree of certainty, depending on the type of information at issue and the harm that would result from unauthorized deletion. The more sensitive the information or the greater the potential harm, the more certainty is required.

d) Requirements Pertaining to Minors

The regulations provide additional requirements for companies that knowingly collect personal information of children 16 and under, with even more requirements for companies that knowingly collect information for children under the age of 13. These requirements are in addition to those mandated by the federal Children's Online Privacy Protection

Act ("COPPA"). In light of the new requirements, companies should perform a detailed inventory of data they collect to determine whether they are subject to the additional regulations pertaining to minors.

e) Recommendations Going Forward

The CCPA prevents the attorney general from enforcing the regulations until July 1, 2020, or six months after the final regulations are published, whichever is sooner. However, companies should not wait to implement changes. The draft regulations underscore the need for companies to work swiftly to review their current policies and procedures and quickly become compliant with the myriad of new requirements in the CCPA. In particular, companies should review what information they collect, and who they collect that information from. Companies should also think hard about how they best can receive consumer requests, verify requesters, and train their employees on responding to requests, especially in light of the tight deadlines imposed by the regulations and the act. While it is possible that the regulations promulgated in the Spring of 2020 could differ, the attorney general will expect companies to be fully compliant with the draft regulations by the time the final version is published.

TransRe
cyber
We value risk.

	Underwriting ▼	Actuarial ▼	Claims ▼
New York	**Elizabeth Geary** **T:** 1 212 365 2243 **E:** egeary@transre.com	**Joseph Marracello** **T:** 1 212 365 2159 **E:** jmarracello@transre.com	**Peter Cridland** **T:** 1 212 365 2032 **E:** pcridland@transre.com
	Miguel Canals **T:** 1 212 365 2266 **E:** mcanals@transre.com		
	Alex Bustillo **T:** 1 212 365 2376 **E:** abustillo@transre.com		
London	**Rhett Hewitt** **T:** 44 (0)20 7204 8676 **E:** rhewitt@transre.com		**Calum Kennedy** **T:** 0207 204 8645 **E:** ckennedy@transre.com