Insurance Coverage Cases Involving Cyber Risks: Survey and Update

Charting a course based on the current cyber coverage horizon suggests a "steady as she goes" approach.[1] Over the last several months, "computer fraud" types of coverages, most often included in commercial crime policies, have produced more decisions and rulings than stand-alone cybersecurity/privacy coverages.

To date, the majority of cases that have addressed potential coverage for data security incidents have involved comprehensive general liability (CGL) policies,[2] where such coverages do not include express terms for "cyber" incidents, "data breaches" or "privacy breaches" but typically include some kind of invasion of privacy language or property damage terms and provisions.[3] There may be an expectation that CGL clashes will start to fade because of the introduction of "cyber" or "data breach" exclusions within those terms.[4] A recent decision involving D&O coverage may also foretell the next *wave* of disputes. We examine these trends below.

Lay of the Land

Exploring the Expanse of CGL

Many of the earlier cases that involved policyholders looking for coverage for data losses or privacy-related events sought defense or recovery further to their CGL policies.[5] Courts wrestled with issues involving "tangible property" provisions and "impaired property" exclusions in the face of allegations that some types of software impaired performance of systems, or that tracking software potentially invaded consumers' privacy.[6] Other courts grappled with property policy terms and power outage events, where the events did not result in "physical damage" but did involve some loss of use or functionality.[7] The next succession of cases involved loss of personal information and whether the event constituted "publication," which amounted to a violation of a person's right to privacy, and thus fell within the personal and advertising injury provisions of CGL terms.[8]

Despite a mixed body of case law and the advent of specific coverages that address breach, loss of data and/or privacy circumstances, given the amounts at issue and the disruptive nature of the events, many policyholders continue to pursue their CGL insurers for recovery.[9] The evolving nature of the threats has also resulted in claims to other types of policies, which in turn has generated fact patterns of first impression and case law that tests the reach of such terms.

Casting About

The Lure of Crime Coverage

With the rise in PHISHING[10] attacks, including SPEAR PHISHING and WHALING, there has been an increase in the number of policyholders seeking recovery for such losses under commercial crime types of policies.[11] The attacks typically involve an email scam or SPOOFING, where an intruder sends a bogus email purported to be from an authority figure to induce someone in an organization to wire funds from a legitimate bank account to an illegitimate or unauthorized account.[12] From the recent court rulings, it appears that the emphasis will be on exactly how the scam was carried out.

For instance, the District Court in *Medidata Solutions, Inc. v. Federal Insurance Company*[13] took pains to comb through the details of the hacker's methodology in order to fit those actions into the Insurer's "computer fraud" and "funds transfer fraud" coverages. Following a SOCIAL

ENGINEERING scam perpetrated against the Insured, in which the Insured wired funds in excess of $4.7 million to a scammer, the Insured sought coverage under its "Federal Executive Protection" policy, under which the terms included a "Crime Coverage Section," with specific provisions for "Forgery," "Computer Fraud" and "Funds Transfer Fraud." The Insurer denied coverage stating that there had been no "fraudulent entry of Data into Medidata's computer system." The Insurer explained that the subject emails were sent to email addresses open to the public, and thus fictitious emails were "authorized." The Insurer argued that there was no coverage under the Computer Fraud coverage, as there was no "manipulation" of the Insured's computers.[14] With respect to the Funds Transfer Fraud coverage, the Insurer argued that the bank wire transfer was "voluntary" and with the Insured's knowledge and consent.[15]

The Court found coverage for the Insured's loss under the Computer Fraud and Funds Transfer Fraud coverages.[16] The Court distinguished other cases interpreting similar Computer Fraud clauses on the facts.[17] The Court noted that "(i)t is undisputed that the theft occurred by way of email spoofing" (as compared to a health insurance company defrauded by healthcare providers who entered claims for reimbursement of services that were never rendered, i.e., "authorized users" entering fraudulent content).[18] The Court found that "(t)o mask the true origin of the spoofed emails, the thief embedded a computer code;"[19] again, as compared to cases where there was "authorized" access to a system, or a loss as a result of a spoofed email sent from a client.[20]

With respect to the Funds Transfer Fraud coverage, the Court found the Insurer's argument that the transfer was "voluntary" to be of no merit. The Policy defined "Funds Transfer Fraud" as "fraudulent electronic . . . instructions . . . purportedly issued by an Organization, and issued to a financial institution directing such institution to transfer, pay or deliver Money . . . from any account maintained by such Organization . . . without (its) knowledge or consent." The Court again distinguished other cases factually by noting that in this case, a third party masked themselves as an authorized representative and directed the Insured's employee to initiate the electronic transfer, which employee would not have initiated the transfer but for the third parties' "manipulation of the emails."[21]

The Court dispensed with the Forgery coverage in quick fashion. The Court found the "absence of a financial instrument (to be) fatal to Medidata's claim for coverage" under the Forgery provision.[22]

In another recent decision, *American Tooling Center, Inc. v. Travelers Casualty and Surety Company of America*,[23] a different District Court analyzed the specific method used to perpetrate the fraud. In *American Tooling*, as part of their usual custom and practice, the Insured's treasurer requested invoices from one of its vendors and received an email response, which appeared to be from their usual vendor but, in fact, the respondent was some other third party (the fraudster – who employed a similar looking email address to the vendor, i.e., deceptive PHISHING as compared to CEO SPOOFING).

The Court noted that the Insured did not make any attempt to verify a change in bank accounts, which the responding "vendor" had requested. The Court considered whether this situation was a "direct loss" that was "directly caused by the use of a computer," as required by the Policy terms, and then noted that there were "intervening events between the receipt of the fraudulent emails and the (authorized) transfer of funds." As such, citing policy language, the Court concluded there was no "direct" loss "directly caused" by the use of any computer:[24]

> *Although fraudulent emails were used to impersonate a vendor and dupe (the Insured) into making a transfer of funds, such emails do not constitute the "use of any computer to fraudulently cause a transfer." There was no infiltration or "hacking" of ATC's computer system. The emails did not directly cause the transfer of funds; rather, ATC authorized the transfer based upon the information received in the emails.*[25]

The perpetrator's "manipulation" method appears to matter, not the fact that there was some kind of loss as a result of a so-called "fraudulent transfer," according to this line of cases.[26] Other courts have noted that where "the fraudulent transfer was the result of other events and not directly by the computer use" (e.g., there was a call to an accounts payable employee), the loss has been deemed not to result "directly" from fraudulent computer use.[27]

Making Headway

Cyber Terms under Scrutiny

Where there have been challenges to terms that include specific cyber, technology or privacy coverages, not surprisingly, Courts have not been shy about taking a deep-dive into the terminology and its application to the technical circumstances under review. In *P.F. Chang's China Bistro, Inc. v. Federal Insurance Company*,[28] a federal court reviewed whether payments by the Insured for certain bank "assessments" following a data breach

were excluded under a "cyber" policy form, further to a contractual exclusion. While there was potential coverage for certain costs asserted by Chang's credit card issuing banks, the Court found that the fees assessed arose only as a result of the Insured's contractual arrangement with the issuing banks.

Matters involving the Telephone Consumer Protection Act ("TCPA") have a tendency to bring out a heightened level of inquiry when it comes to the Insured's actions and how the allegations of wrongful conduct potentially implicate cyber terms.[29] One Illinois Court looked carefully at the alleged statutory violations (TCPA, Consumer Fraud Act) to see whether such allegations fell within a "privacy wrongful act" definition. The Court concluded that because these regulations were not connected with the "control or use of personally identifiable financial, credit or medical information," the controlling terms in the Policy, there was no obligation for the Insurer to defend the Insured.[30]

By comparison, one Court did not have to wade in too deep into its analysis when asked to consider whether accusations of "withholding data" fell within the cyber terms.[31] In a coverage action initiated by the cyber Insurer, the Court agreed that the allegations against the Insured were not the result an "error, omission, or negligence." As such, there was no uncertainty whether a defense obligation arose because the allegations only addressed intentional conduct.[32]

What is considered "data" was the subject of a court's analysis of an exclusion in a multimedia policy.[33] In a ruling on summary judgment motions, the Court noted that "television programming" did not fit within the meaning of data, where the terms excluded claims arising out of "unauthorized access to, unauthorized use of, or unauthorized alteration of any computer or system . . . data . . . (including the introduction of malicious code/virus by any person)."

Another court dipped back into the "publication" waters in analyzing whether posting medical records on the Internet was "electronic publication." Referencing some of the CGL cases previously discussed, the court answered this question in the affirmative.[34]

Another cyber coverage dispute puts a spotlight on specific security issues that became apparent following a data breach.[35] Reportedly, the breach exposed confidential health records of patients, whose information was stored on a system accessible via the Internet, and not protected by encryption or other measures. In *Columbia Casualty v. Cottage Health*, the Policy included an exclusion for "Failure to Follow Minimum Required Practices," which the Insurer raised following settlement of the class action lawsuit but while certain regulatory investigations were ongoing.[36] The exclusion states:

> based upon, directly or indirectly arising out of, or in any way involving:
>
> 1. Any failure of an Insured to continuously implement the procedures and risk controls identified in the Insured's application for this Insurance and all related information submitted to the Insurer in conjunction with such application whether orally or in writing;
>
> 2. Failure to follow (in whole or part) any Minimum Required Practices that are listed in Minimum Required Practices Endorsement; or
>
> 3. The Insured's failure to meet any service levels, performance standards or metrics;

Per an endorsement, the Policy contained an "exception" to the exclusion, stating that the exclusion shall not apply to:

> 1. an Insured Person's negligent circumvention of controls; or
>
> 2. an Insured Person's intentional circumvention of controls where such circumvention was not authorized by the Insured;
>
> 3. Insured Entity's upgrade or replacement of any procedure or control in item 1 above if the upgrade or replacement procedure or control is at least as effective as the one it replaces.

The Insured filed its own action against its Insurers and, in that lawsuit, the Insured makes a specific reference to the exceptions to the "minimum required practices" exclusion; although, for now, the Insured's allegations do not specify how the underlying class action allegations, or any facts relating to the regulatory actions, for that matter, unavoidably fit within the language of any the exceptions.

The Insurer's latest complaint likewise speaks to the exception language. The Insurer alleges that its investigation "revealed that the breach was not caused by `an Insured Person's' negligent or intentional but unauthorized circumvention of controls, or by Cottage's `upgrade or replacement' of any of the procedures or risk controls described in the application but, rather, by the complete absence of any such risk controls in the first instance." The Insurer alleges, in part, that the breach was caused by the Insured's "failure to continuously

implement the procedures and controls identified" in the application, and cites a failure to replace default (security) settings (easier to hack, presumably), and a failure to ensure that the Insured's systems were securely configured. For now, the default setting issue appears to be the most specific fact raised as part of the dispute over whether the Insured met its purported security obligations.

Ostensibly, debating these points likely will require expert witness testimony as to the Insured's security practices and protocol. Ultimately, any court rulings with respect to the exclusion language will scrutinize the "minimum practices" and reconciling likely competing and, even more likely, highly technical evidence.

Other skirmishes over cyber terms are afloat and involve questions relating to "trade secrets" and media content (digital music content), allegations of FACTA violations, and findings of fraudulent misrepresentations in technology services.[37] Some true "cyber coverage" disputes have been resolved without any courts having to weigh in on the specific language in those coverages, despite the frothy issues at stake (payments to credit card brands following intrusion into payment processing system; whether PCI assessments should fall within the full limit, potentially as damages, instead of a specified PCI sublimit).[38]

A Hard Tack

Chasing D&O and Other Sources

In yet another TCPA case, the Ninth Circuit recently found that the Los Angeles Lakers were not owed a defense under its Directors and Officers coverage, because the terms included an "invasion of privacy" exclusion.[39] These terms stated that the Insurer excluded claims "based upon, arising from, or in consequence of . . . invasion of privacy," but did not specifically reference the TCPA. Therefore, the Court first analyzed whether the TCPA was to prevent invasions of privacy or some other harms, and found that "in pleading the elements of a TCPA claim, a plaintiff pleads an invasion of privacy claim."[40] Thus, the Court found that Plaintiffs' two claims, negligent and willful TCPA violations, fell within the exclusion, while acknowledging that "exclusionary clauses are to be construed against the insurer" as well as noting the broad scope of a duty to defend. The Los Angeles Lakers have since filed a petition for *en banc* review which has been supported by policyholder advocates.

Payments pursuant to Merchant Services Agreements following a data breach continue to be a source of consternation for policyholders. Where a retailer suffered a data breach of its credit card payment system, it was subject to having its daily payment card settlements withheld by the financial institution that serviced the credit card brands.[41] The financial institution also issued a "demand" that the retailer should improve its security. Effectively the credit card brands levied or potentially could levy fines against the financial institution, which then would be recovered from the retailer per the merchant agreement terms.

The retailer filed suit against this financial institution, asserting breach of contract. The retailer notified its Insurer further to a Privacy Company Management Liability policy, which includes a Directors, Officers and Corporate Liability Coverage. The Insurer declined to pay litigation expenses for the Insured's suit over the withheld funds. The Insurer raised a contract exclusion, among other issues. The Insured sought declaratory relief, asserting that the Policy obligated the Insurer to defend.

While the Court found that the so-called "demand" letters from the financial institution potentially fell within the definition of "claim," the Court declined to impose a defense obligation on the Insurer.[42] The Court found that contract exclusion applied under the circumstances. The Court noted that the demand letters state that the claims against the retailer were based only in contractual indemnification terms and the Court rejected the notion that the liability arose separate and apart from those terms.[43]

Again, given the sums at issue (which in the above example were in excess of $4 million), it seems natural for a policyholder to press coverage under any and every available terms – even homeowners' policies (accountant lost laptop case; client had to send out notifications, sought recovery under the actual individual accountant's homeowner policy; court found no duty to defend).[44]

Sally Forth

Vistas Coming into View

One common theme from the above survey is that as the cyber attacks become more creative as well as more prevalent, more pressure will be brought to bear on managing and offsetting the risk. Many of the most recent rulings reveal that courts will endeavor to strip down the elements of the attack, or the Insured's conduct, to see how the wrongful acts line up with the

coverage terms. Finally, given these pressures, we would anticipate an upswing in the very near future of decisions and rulings that address true "cyber" terms.

Contacts:

Kevin G. Flynn
kevin.flynn@mendes.com
1.212.261.8321

Margaret A. Reetz
margaret.reetz@mendes.com
1.212.261.8726

Allen E. Sattler
allen.sattler@mendes.com
1.212.261.8452

Lauren B. Prunty
lauren.prunty@mendes.com
1.212.261.8303

Gregory S. Mantych
gregory.mantych@mendes.com
1.212.261.8091

Editor:
Douglas Giombarrese
douglas.giombarrese@mendes.com

[1] With a nod to the *cyber at sea* crew, per the old adage, "Red sky at night, sailors' delight. Red sky in morn, sailors take warn." The rhyme is a rule of thumb used for weather forecasting during the past two millennia. It is based on the reddish glow of the morning or evening sky, caused by haze or clouds related to storms in the region. http://www.metoffice.gov.uk/learning/learn-about-the-weather/how-weather-works/red-sky-at-night. For recent cyber at sea developments, see *Be Cyber Aware at Sea*, a maritime and offshore industry initiative, which includes a newsletter entitled "Phish & Ships." https://www.becyberawareatsea.com/awareness. "Red sky in morn:" the *NotPetya* attack reportedly will cost Maersk $300m. https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html

[2] ISO standard CGL policy form, divided into three main parts: Coverage A: Bodily Injury and Property Damage Liability; Coverage B: Personal and Advertising Injury Liability; and Coverage C: Medical Payments. Ins. Serv. Office, Inc., Form 00 01 12 07, at 1-9 (2006).

[3] *See, e.g.*, Am. Guarantee & Liab. Ins. Co. v. Ingram Micro, 2000 WL 726789 (D.Ariz. Apr. 18, 2000) (power outage knocked out systems, causing loss of data, software functionality; court found there was "property damage" per CGL terms); Eyeblaster, Inc. v. Fed. Ins. Co. 613 F.3d 797 (8th Cir. 2010) (Insured was sued over allegations that its advertising tracking software installed spyware on non-consenting Plaintiff; allegations included invasion of privacy, deceptive practices; District Court granted Insurer summary judgment but Appellate Court found "loss of use" of computer allegations fell within "tangible property" terms of GL policy; *compare,* America Online, Inc. v. St. Paul Mercury Ins. Co., 347 F.3d 89 (4th Cir. 2003), which found that data, information, instructions are not "tangible property," and "impaired property" exclusion precluded coverage for loss of use of tangible property that is not physically damaged); Zurich Am. Ins. v. Sony Corp. of Am., 2014 N.Y. Misc. LEXIS 5141 (N.Y. Sup. Ct. 2015) (insured sought coverage under CGL terms for alleged transmission of private information by hackers); Recall Total Information Management Inc. v. Federal Insurance Co., 2015 WL 2371957 (Conn. May 26, 2015) (personal employment data stored on computer tapes for IBM past/present employees was lost in transit, when the tapes fell out of the back of a van; IBM pursued transport carrier's CGL insurers; court held IBM's losses were not covered by the personal injury clauses of the CGL policies because there had been no "publication" of the information stored on the tape).

[4] In 2014, ISO introduced endorsements addressing the access or disclosure of confidential or personal information; CG 21 06 05 14 (Exclusion – Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability – With Bodily Injury Exception) (Excludes coverage, under Coverages A and B, for injury or damage arising out of any access to or disclosure of any person's or organization's confidential or personal information; limited bodily injury exception); CG 21 07 05 14 (Exclusion – Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability – Limited Bodily Injury Exception Not Included); http://www.insurancejournal.com/news/east/2014/07/18/332655.htm

[5] *See* Ingram Micro; Eyeblaster, America Online, etc., *supra* note 3.

[6] *See* America Online *supra,* note 3; *see also,* Retail Systems, Inc. v. CNA Insurance Company, 469 N.W.2d 735 (Minn.Ct.App. 1991) (computer tape and data integrated completely with physical property; court found coverage under CGL as "tangible property").

[7] See, Ingram Micro *supra,* note 3 (electrical outage, where Insurer said there was no "physical damage" further to "all risks" policy language: "(a)ll Risks of direct physical loss or damage from any cause…"; but, court found

"physical damage" is not restricted to physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality); *see also,* NMS Services, Inc. v. Hartford Insurance Company, 62 Fed. Appx. 511 (4th Cir. 2002) (property coverage with computer and media endorsement; court found acts of destruction by employees do not preclude coverage); *compare,* Ward General Ins. Serv., Inc. v. Employees Fire Ins. Co., 114 Cal.App.4th 548 (2003) (no coverage for costs of recovery of data or business interruption; no loss of or damage to tangible property).

[8] Tamm v. Hartford Fire Ins. Co., Mass. Super. LEXIS 214 (Mass. Super. Ct. 2003) (insurer owed duty to defend per "personal injury" provision where former employee threatened to disseminate information from private e-mail accounts); *see also,* Zurich *supra*, note 3 (where allegedly personal information of Insured's customers was stolen, following a hacking incident; court found no coverage because Insured had not published the information); Creative Hospitality Ventures, Inc. v. United States Liab. Ins. Co., 444 Fed. Appx. 370, 375-76 (allegations of violations of Fair and Accurate Credit Transactions Act, FACTA; appellate court held that providing a customer with a receipt revealing the customer's own account information was not "publication" for CGL purposes); Cynosure In. v. St. Paul Fire & Marine Ins. Co., 645 F.3d 1, 2 (1st Cir. Mass. 20111) (invasion of privacy provision under Coverage B referred to "disclosure, not intrusion;" no coverage for underling civil action involving BLAST FAXES, alleged violations of TCPA, Telephone Consumer Protection Act).

[9] *See,* American Economy Insurance Co., et al. v. Aspen Way Enterprises Inc., et al., case number 16-35059 (9th Cir. May 26, 2017) (affirmed District Court ruling that Insurers had no duty to defend lawsuits that alleged Insured's franchisee sold or rented software programs that enabled the company to spy and monitor users' personal information; no coverage under CGL terms that contain "recording and distribution" exclusion, which precludes coverage for any suit alleging a violation of a federal statute that prohibits the transmitting or distribution of material/information; further, there was no "publication" to trigger coverage under personal and advertising injury terms); National Fire Ins. Co. of Hartford, et al. v. E. Mishan & Sons, Inc., Case No. 15-2248 (2nd Cir. June 1, 2016), Summary Order (defense obligation under CGL terms for class action lawsuits alleging TCPA violations, as a result of allegedly trapping customers into recurring credit card charges, transferring private customer information for profit); *see also,* St. Paul Fire & Marine Ins. Co. v. Rosen Millennium, Inc., Case No. 6:17-cv-00540-CEM-GJK (complaint recently filed; Insurer disclaims coverage under CGL terms for payment card brand fines, PCI-DSS assessments, following a data breach; seeks declaratory relief); Hartford Casualty v. Corcino & Assoc., Case No. CV 13-3728 GAF (C.D. Calif. Oct. 7, 2013) (Insurer issued CGL policy that included obligation to pay because of "electronic publication of material that violates a person's right of privacy," with exclusion for violations of state/federal acts; court found coverage obligation because right to medical privacy was not solely created by statutes).

[10] Additional information on all terms in SMALL CAPS throughout the article can be found in the Glossary, attached.

[11] "According to Wombat Security Technologies' State of the Phish report, 76% of infosecurity professionals still report that their organizations have been victims of a PHISHING attack this year. Half (51%) said the rate of attacks is increasing." https://www.infosecurity-magazine.com/news/phishing-awareness-grows-but/

[12] *See also*, Bitpay, Inc. v. Mass. Bay Ins. Co., Case no1:15-cv-03238 (N.D. Ga. Mar. 17, 2016), *dismissed with prejudice* (description of SPEAR PHISHING attack on a bitcoin payment processor's CFO; attacker infiltrated email of someone CFO had a prior business relationship with; directed CFO to website controlled by hacker; captured CFO's credentials and fraudulently transferred bitcoin; Insurer denied coverage under

"Computer Fraud" provision stating "(t)he facts…do not support a direct loss since there was not a hacking or unauthorized entry into (Insured's) computer system fraudulently causing a transfer of Money.")

[13] Case No. 15-CV-907 (ALC), *Memorandum and Order Granting Summary Judgment*, (SDNY, July 21, 2017) (notice of appeal filed by Federal) (Medidata notified its finance department of company's possible acquisition and instructed finance personnel "to be prepared to assist…on an urgent basis;" account payable employee received email shortly thereafter purporting to be from the company's president, instructing employee re: upcoming acquisition, identifying lawyer, and employee received call from purported lawyer, and then a group email purportedly from company president directing wire transfer of $4.7 million; subsequent attempt raised suspicions because of how president's email looked; the actual president said he had not requested funds; FBI notified; investigations revealed an unknown actor had altered the emails that were sent to the president to make them appear as if they were sent from company president).

[14] *Id.* at 8.

[15] *Id.* at 14.

[16] *Id.* at 15.

[17] *See,* Universal Am. Corp. v. Nat'l Union Fire Ins. Co., 25 N.Y.3D 675 (2015); Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am., No. 13-CV-5039 (JFW), 2014 WL 3844627 (C.D. Cal. July 17, 2014).

[18] *See,* Universal, at 680-81, where Court of Appeals held that the policy "applie(d) to losses incurred from unauthorized access to Universal's computers system, and not to losses resulting from fraudulent content submitted to the computer system by authorized users."

[19] *Medidata* at 10.

[20] *Id.* at 11, "The thief's computer code (in *Medidata*) also changed data from the true email address to Medidata's president's address to achieve the email spoof," as compared to the fraud committed in *Pestmaster*, a payroll administrator's withdrawal of funds from a corporation's bank account; or, in comparison to theft directly from an accounting firm, where the thief disguised himself as the client in Taylor & Lieberman v. Fed. Ins. Co., No. 14-CV-3608 (RSWL (SHX), 2015 WL 3824130 (C.D. Cal. June 18, 2015).

[21] *Medidata*, at 15, as compared to instances where an authorized transfer was made for fraudulent purposes, or a "voluntary" transfer was made which subsequently was determined to be a part of a fraudulent scheme, i.e., Bernie Madoff; "larceny by trick is still larceny."

[22] *Id.*

[23] Case No. 5:16-cv-12108-JCO-APP (Ea. Dist. Mich. Aug. 1, 2017).

[24] *Id.* at 5. The Court distinguished this case from *Medidata* on the basis that the policy language differed. Specifically, the policy language at issue here included language requiring a "direct loss" to be "directly caused by the Computer Fraud" whereas the policy in *Medidata* did not.

[25] *Id.* at 7, citing *Pestmaster*, "the phrase `fraudulently cause a transfer to' to `require the unauthorized transfer of funds." "Because computers are used in almost every business transaction, reading this provision to cover all transfers that involve both a computer and fraud at some point in the transaction would convert this Crime Policy into a `General Fraud' Policy;" and *see also,* Incomm Holdings, Inc. v. Great American Ins. Co., 2017 WL 1021749*10 (N.D. Ga. Mar. 16, 2017) (program manager for a "chit" redemption system for prepaid debit cards was the victim of a scheme where cardholders were able to obtain more credit than that to which they were originally entitled or paid; with the aid of a flow chart of the redemption process laid out in the opinion, the Court found that under the "computer fraud" provision of the Policy, there was no "computer" "use." Instead the Court

noted that the fraud was committed using telephones and not computers. The Court further found that the loss did not result "directly" from any computer use) (Insured filed its notice of appeal June 13, 2017).

[26] See *also* description of similar VISHING type of fraud and how a Canadian court analyzed how the fraud was committed when applying "computer fraud" terms; https://www.bennettjones.com/CybersecuritySpearPhishingCoveredUnderInsurancePolicyWhereCodeManipulated; http://www.dandodiary.com/2017/08/articles/cyber-liability/guest-post-first-canadian-cyber-coverage-decision-joins-series-u-s-judgments-social-engineering-frauds/

[27] *See* Apache Corp. v. Great Am. Ins. Co., *No. 15-20499, 2016 WL 6090901, 2016 U.S. App. LEXIS 18748 (5th Cir. Oct. 18, 2016)*(a caller claiming to be a vendor contacts an accounts payable employee, requesting account change for future payments; employee says put it in writing, "on official letterhead;" "caller" sends email with letter on "official letterhead," with caller's number; Insured "verifies" request and sends $2.4 million to fraudster; Court found that the loss did not result directly from the computer fraud because "The email was part of the scheme; but, the email was merely incidental to the occurrence of the authorized transfer of money."); *see also,* Aqua Star (USA) Corp. v. Travelers, 2016 WL 365565 (W.D. Wash. July 8, 2016) (Court found that "Electronic Data" exclusion in crime policy applied because the "entry of Electronic Data into Aqua Star's Computer System was an intermediate step in the chain of events that led Aqua Star to transfer funds to the hacker's bank accounts. Because an indirect cause of the loss was the entry of Electronic Data into Aqua Star's Computer System by someone with authority to enter the system, Exclusion G applies."); *Compare,* Principle Sols. Grp., LLC v. IronShore Indem., Inc., No. 1:15-CV-4130-RWS, 2016 WL 4618761, at *2 (N.D. Ga. Aug. 30, 2016)(email from person purporting to be one of the Insured's managing directors; instructs controller to work with an outside attorney to ensure that a wire "goes out today:" controller receives email from "lawyer," with wire instructions for a bank in China; controller confirms instructions in a phone call with "lawyer" and relays information to financial institution; the next day, the real director said he had no knowledge of emails, lawyer, wire; Insured sought coverage under Commercial Crime Policy, with Computer and Funds Transfer Fraud" provision; District Court on summary judgment found in favor of the Insured, disagreeing with Insurers' contention that the wire transfer did not result "directly" from the "fraudulent instruction;" the Court stated that the Insured "could act only through its officers. If some employee interaction between the fraud and the loss was sufficient to allow (the Insurer) from paying under the provision at issue, the provision would be rendered 'almost pointless' and would result in illusory coverage," citing the District Court's language from *Apache*; note also, that the coverage terms stated Insurer will pay for loss "resulting directly from a 'fraudulent instruction' directing a 'financial institution' to debit" the Insured's account, which language differs from *American Tooling*'s language, "pay for loss… directly caused by… use of any computer to fraudulently cause a transfer"); and *see,* State Bank of Bellingham v. BancInsure, Inc. No. 14-3432, --F.3d--, 2016 WL 2943161 (8th Cir. May 20, 2016) – (coverage for fraudulent wire transfer under a Financial Institution Bond form – "the efficient and proximate cause' of the loss…was the illegal transfer of the money and not the employees' violations of policies and procedures," where bank employee left computer "running" overnight and discovered fraudulent wire transfers the next day).

[28] 2016 WL 3055111 (D. Ariz. May 31, 2016).

[29] Telephone Consumer Protection Act 47 U.S.C. § 227

[30] Doctors Direct Ins., Inc. v. Bochenek, 2015 IL App (1st) 142919, 38 N.E.3d 116 (The Court also declined to find that the mere fact that a list of potential customers was allegedly transferred from a spa to a medical provider rendered such

a list "personally identifiable medical information." Many cyber terms have references beyond "financial, credit or medical information" in relation to what may be considered personally identifiable information.)

[31] *Travelers Property Casualty Company of America, et al. v. Federal Recovery Services, Inc., et al* (Case No. 2:14-CV-170 TS);

[32] *See also, Life*Lock, Inc. v. Certain Underwriters at Lloyds, 2017 WL 161045 (N.Y. App. Div. Jan. 17, 2017) (Insured sought coverage per media/privacy policy for class actions alleging Fair Credit Reporting Act violations; Insurer successfully cited exclusions for prior acts, wrongful conduct pre-dated retroactive date, and unfair trade practices).

[33] Ellicott City Cable, LLC v. Axis Ins. Co., No. RDB-15-02506 (D. Md. July 22, 2016) ("data" in the context of the Axis policies, "appears to concern information related to the internet, not television programming.")

[34] The Travelers Indemnity Company v Portal Healthcare Solutions, L.L.C., Case No. 14-1944 (4th Cir. April 11, 2016), *unpublished opinion* (affirmed ruling of District Court, which found that the Insurer had a duty to defend class actions alleging that confidential medical records were posted on the Internet, and therefore were "published" under the policy's personal injury, advertising injury and website liability coverage).

[35] Columbia Casualty Co v Cottage Health System, 2:15-c v-03432 (CD Cal 2015) (the original declaratory action filed by the Insurer was dismissed pursuant to the Insured raising the Policy's ADR provision; the parties engaged in an unsuccessful mediation and both immediately filed suit upon expiration of the "cooling off period;" Insured moved to dismiss the federal court action in favor if its state court action and the federal district court agreed; the Insurer has appealed that ruling, *see* Columbia Casualty v. Cottage Health, Case No. 16-56872 (9th Cir.); *see also,* Cottage Health v. Columbia Casualty Company, Certain Underwriters at Lloyd's London, Case No. 16CV02310 (Cal. Super. Ct., Santa Barbara County); *compare*,

[36] Columbia Casualty Co v Cottage Health System, 2:15-c v-03432 (CD Cal 2015)

[37] *See, e.g.,* Certain Underwriters at Lloyd's, London v. Wunderland, 2015-CH-18139 (Cir. Ct. Cook County, Ill.) (in a dispute over non-compete terms, did allegations of misappropriation of trade secrets arise out of media or user-generated content, under Cyber, Privacy and Media Risks policy); *AIG Specialty v. Laboratory Corporation of America Holdings,* Case 0:17-cv-6159-BB 9 (So. Dist. Fla. 2017)(whether alleged willful violations of FACTA – Fair and Accurate Credit Transactions Act – includes any claim for "damages" since Class Action Plaintiffs only sought statutory amounts); Illinois National Insurance v. Experian Information Solutions, Case No. 17-cv-6668 (No. Dist. Ill. Sept. 15, 2017) (Insurer seeks declaratory relief that tech professional services Policy terms do not respond to findings of fraudulent misrepresentations).

[38] State National Insurance Company v. Global Payments, Inc., Case No. 1:13-cv-01205 (No. Dist. Ga. Dec. 14, 2013) (settled); New Hotel Monteleone, LLC v. Certain Underwriters at Lloyd's of London, Case No. 2015-11711 (Civil District Court for the Parish of Orleans), removed to U.S.D.C, Case No. 2:16-cv-00061-ILRL-JCW (Insured alleged that it purchased cyber coverage after one cyber-attack, and expected that a full policy limit should apply to PCI assessment rather than sublimit; following removal to federal court, placing broker brought third-party action against wholesaler, alleging that it had advised the wholesale broker of the earlier attack, involving "fraud recovery and operational reimbursement" from credit card brands, and that it relied on wholesaler's expertise re: cyber coverage; case dismissed with prejudice.)

[39] Los Angeles Lakers, Inc. v. Federal Insurance Company, (2017) 9th Cir. No. 15-55777.

[40] *Id. at 14.*

[41] Spec's Family Partners v. The Hanover Insurance Company, Case 4:16-cv---438 (So. Dist. Tx., Mar. 15, 2017)

[42] *Id.* at 8.

[43] *Id.* at 13.

[44] *See,* Nationwide Insurance Company v. Jeanne Hentz, et al., Case No. 3:11-cv-00618-JPG-PMF (So. Dist. Ill. March 6, 2012) (exclusion for coverage for property damage in the care of the insured applied).

Glossary

(Cyber Attacks)

ADWARE - intent is primarily to display advertising content on your computer. Often using pop-up windows, adware programs flash advertisements and links to other websites.[1]

BAITING - the promise of an item or good that hackers use to entice victims; offer users free music or movie downloads, if they surrender their login credentials to a certain site; [2]

BLAST FAXING – Unsolicited advertisements sent to a fax machine, sometimes called "junk faxes." In most cases, FCC rules under the Telephone Consumer Protection Act and Junk Fax Prevention Act prohibit sending junk faxes;[3]

CEO SPOOFING - e-mail scams in which the attacker spoofs a message from the boss and tricks someone at the organization into wiring funds to the fraudsters (sometimes referred to as "fake president fraud");[4] CEO fraud generally involves some form of business email compromise (BEC), spear phishing attack or whaling scam in which a series of bogus emails from a company's CEO, CFO or other senior executive persuade the targeted employee to quickly transfer funds into fraudulent accounts in a manner that bypasses the usual safeguards. Unlike conventional phishing attacks, which are generic and blasted to as many people as possible, CEO fraud emails are much more customized and convincing.[5]

PHARMING – a form of online fraud very similar to phishing as pharmers rely upon the same bogus websites and theft of confidential information. However, where phishing must entice a user to the website through 'bait' in the form of a phony email or link, pharming re-directs victims to the bogus site even if the victim has typed the correct web address. This is often applied to the websites of banks or e-commerce sites. Phishing involves the receipt of an e-mail message that appears to come from a legitimate enterprise.[6] Pharming attacks compromise at the DNS server level, re-directing you to a hacker's site when you type in a company's Web address;[7]

PHISHING – "deceptive phishing:" any attack by which fraudsters impersonate a legitimate company and attempt to steal people's personal information or login credentials;[8]

PRETEXTING - scammer who pretends that they need certain bits of information from their target in order to confirm their identity;[9]

QUID PRO QUO – fraudsters who impersonate IT service people;[10]

SOCIAL ENGINEERING - hackers who exploit the one weakness that is found in each and every organization: human psychology. Using a variety of media, including phone calls and social media, these attackers trick people into offering them access to sensitive information;[11]

SMISHING –uses cell phone text messages to lure consumers in. Often the text will contain an URL or phone number. The phone number often has an automated voice response system. And again, just like phishing, the smishing message usually asks for your immediate attention. In many cases, the smishing message will come from a "5000" number instead of displaying an actual phone number. This usually indicates the text message was sent via email to the cell phone, and not sent from another cell phone.[12]

SPEAR PHISHING – fraudsters customize their attack emails with the target's name, position, company, work phone number and other information in an attempt to trick the recipient into believing that they have a connection with the sender;[13]

SPOOFING - when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity. Spoofing is often used as part of an attempt to trick someone into giving away valuable personal information so it can be used in fraudulent activity or sold illegally;[14]

SPYWARE - software that runs in the background, collecting information or monitoring Internet browsing activities; harvests information related to an individual's computer and how that person uses it;[15]

TAILGATING - attack involves someone who lacks the proper authentication following an employee into a restricted area;[16]

VISHING – fraudsters using the phone to solicit someone's personal information; relies on "social engineering" techniques to trick someone into providing information that others can use to access and use that person's important accounts; also use this information to assume someone else's identity and open new accounts.[17]

WHALING – where fraudsters attempt to harpoon an executive and steal their login credentials;[18] Attackers often gather the details that they need to personalize their attacks from social media such as Facebook, Twitter, and LinkedIn, profiling targets' company information, job details, and name of coworkers or business partners.[19]

---

[1] https://us.norton.com/internetsecurity-how-to-catch-spyware-before-it-snags-you.html
[2] https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/
[3] https://www.fcc.gov/consumers/guides/faqs-about-junk-faxes
[4] https://krebsonsecurity.com/2016/04/fbi-2-3-billion-lost-to-ceo-email-scams/
[5] https://www.pivotpointsecurity.com/blog/ceo-fraud/
[6] https://us.norton.com/cybercrime-pharming;
[7] http://www.zdnet.com/article/phishing-vs-pharming/
[8] https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/
[9] *See supra,* note 2.
[10] *See supra,* note 2.
[11] *See supra,* note 2.
[12] https://security.intuit.com/index.php/protect-your-information/phishing-pharming-vishing-and-smishing
[13] *See supra,* note 2.
[14] https://www.fcc.gov/consumers/guides/spoofing-and-caller-id
[15] *See supra,* note 1.
[16] *See supra,* note 2.
[17] https://security.intuit.com/index.php/protect-your-information/phishing-pharming-vishing-and-smishing
[18] *See supra,* note 2.
[19] https://digitalguardian.com/blog/what-whaling-attack-defining-and-identifying-whaling-attacks