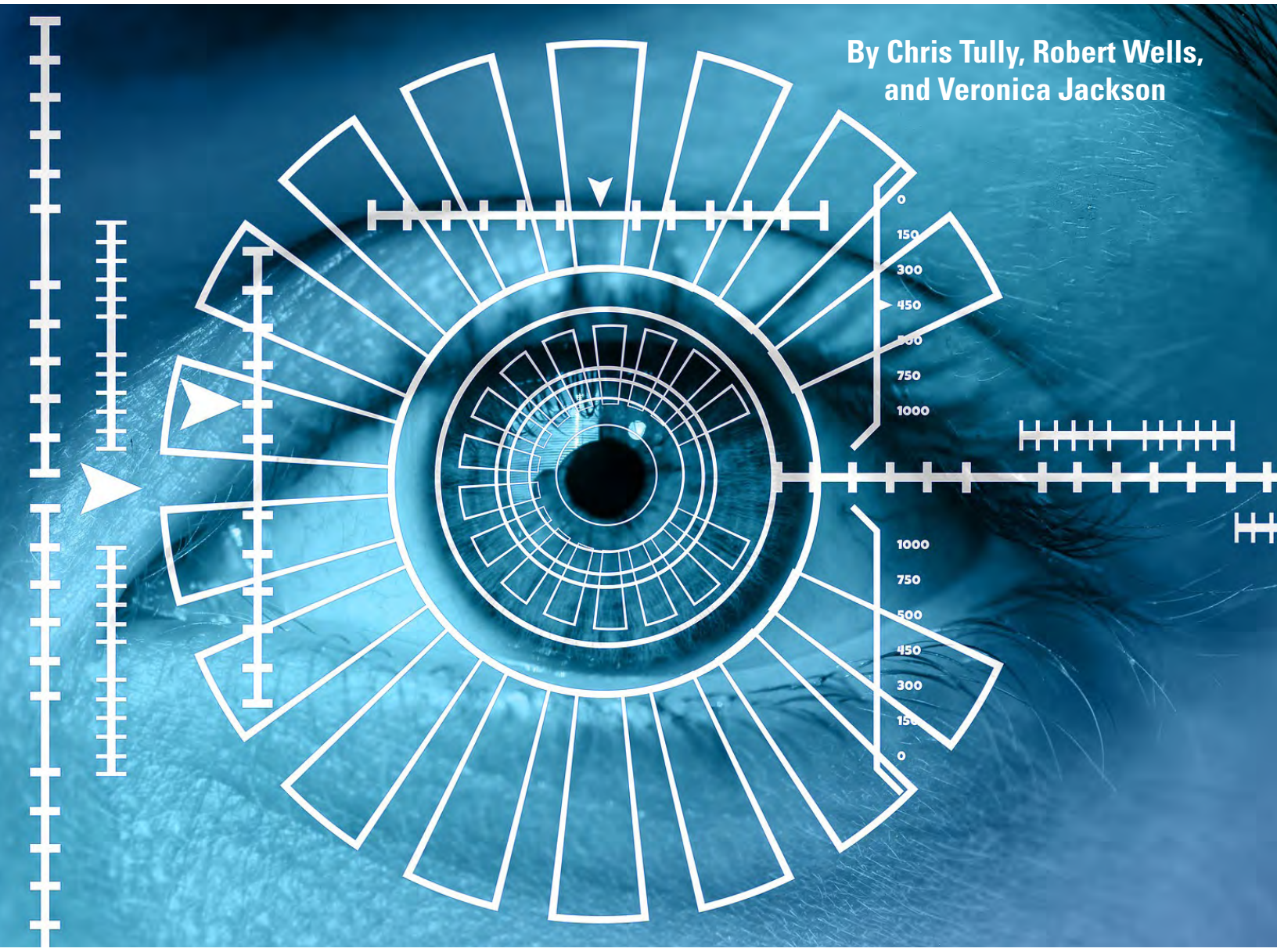
March 2020

THE DEFENSE LINE

A Publication From Maryland Defense Counsel, Inc.

Biometric Data

Companies Should Act to Mitigate Risks in the Face of Growing Regulations and Increased Risk for Liability



By Chris Tully, Robert Wells, and Veronica Jackson

Also Featured

President's Message

Welcome to the almost-Spring edition of *The Defense Line*. Our hard-working editor Sheryl Tirocchi and graphics consultant Brian Greenlee have again done excellent work assembling this issue. We hope you will find it interesting and informative.

This President's Message will be brief, with just a quick recap of current MDC activities. (I always liked John Wayne's advice: "Talk low, talk slow and don't say too much." While those reading this column are spared listening to me talking low and slow, you will probably appreciate the brevity.)

Dwight W. Stone, II, Esquire

Miles & Stockbridge P.C.

With the Maryland General Assembly's legislative session underway, MDC is engaged in Annapolis. We recently held a reception for members of the Senate Judicial Proceedings Committee and the House Judiciary Committee, which was quite well-attended. Many of the members of these important committees are new, and the reception was a good opportunity for MDC legislative leaders to meet and chat informally with them, as well as with the more experienced legislators, and to discuss issues of mutual concern. MDC will also be providing written and oral testimony in Annapolis on various bills that are important to our members and clients. From workers' compensation, to medical malpractice, to general liability and beyond, we are working hard to ensure your voice is heard. If you are interested in becoming involved in MDC's legislative committee, call or email me and we will get you plugged in.

Legislative engagement is just one area in which MDC members can make a difference in the Maryland legal community while enhancing their professional networks. We also have the following active subcommittees and committees: Appellate Practice; Judicial Selections; Workers' Compensation; Publications; Programs; Construction Liability; Commercial Law; Construction; Employment Law; Health Care and Compliance; Lead Paint; and Privacy, Data and Security. And, we will soon be forming a Membership Committee focusing on bringing new MDC members on board and enhancing MDC's value for existing members. If you have interest in joining any of these efforts, please contact me. We offer a lot of interesting opportunities, whether you are a newer attorney or one with decades of experience. To get a more comprehensive view, visit our website: **www.mddefensecousel.org**. For younger attorneys, we offer valuable leadership opportunities that would be difficult to find in other organizations.

Finally, please be on the lookout for our emails notifying you of upcoming "Lunch and Learn" programs and happy hours. We will hold a number of these educational and social events this Spring, and look forward to seeing you in attendance. Of course, we will also hold our famous Crab Feast/Annual Meeting in June — which will be here before we know it.

Get Involved With MDC Committees

To volunteer, contact the chairs at

www.mddefensecounsel.org/leadership.html.

Committees

- Appellate Practice • Judicial Selections • Legislative • Publications
- Programs & Membership • Sponsorship

Substantive Law Committee

- Commercial Law • Construction Liability • Employment Law
- Health Care and Compliance • Insurance Coverage • Lead Paint
- Negligence & Insurance • Privacy, Data, and Security
- Products Liability • Professional Liability • Workers' Compensation

THE DEFENSE LINE

March 2020

The Defense Line is a publication from Maryland Defense Counsel, Inc.

Maryland Defense Counsel
1 South Street, Suite 2600
Baltimore, MD 21202

E-mail:
ed@mddefensecounsel.org
www.mddefensecounsel.org

Cover Photo: Pixabay.com

TABLE OF CONTENTS

Accountants: Be Leery of Requests from Clients' Financial Institutions

Maryan Alexander

With more and more frequency, accountants are asked to provide information, verify their work product, or confirm information about their clients to non-client third-parties such as loan brokers, lenders, insurers, and investors. Some third-parties also request accountants to acknowledge reliance on the information provided in what are referred to as "privity letters", "reliance letters", or "comfort letters." These requests direct the accountant to verify the accountant's work and are used to put the accountant on notice of the third-party's intended reliance. While an accountant owes a duty of due care to the client, a verification request may create a duty to non-client third-parties who claim detrimental reliance on the accountant's work product and expose the accountant to potential liability. When receiving these requests, accounting practitioners should proceed with extreme caution.

Common Scenarios

Potentially problematic requests can come up in connection with a client's pending borrowing or refinancing application, insurance placement, transaction due diligence, or any number of other scenarios. Stricter lending practices have resulted in more lending institutions requesting a borrower's accountant to affirmatively grant privity to the third-party or verify the borrower's income tax returns or financial statements directly to that third-party. Lending institutions sometimes add provisions in loan agreements that require the borrower to "direct" their accountant to provide certain types of information upon request from the lender and accompany that information with a statement confirming the accountant's understanding that the lender will rely on the information to make a credit decision. One example is that insurers sometimes send letters to policyholders' accountants stating that the insurer relied on the accountants' work product in placing the insurance and ask the accountant to acknowledge the insurer's reliance.

The task of assessing an applicant's creditworthiness and verifying the accuracy of the financial information submitted by an applicant should be the exclusive responsibility of the lender, insurer, or other third-party assessing whether to act on the request. Financial institutions making these assessments may find this challenging, particularly when the applicant is self-employed or plans to use a distribution of business assets to fund a down payment or closing costs on a loan. To shift the burden of verifying the borrower's financial information, and also to shift some of the risk to the accountant, creditors try to build a basis for asserting they are in privity with the accountant so they have standing to sue the accountant if the creditor is not repaid. If a borrower later defaults on the loan, the broker or lender may take the position that it detrimentally relied on the accountant's verification and representations in approving the loan to establish a basis to sue the accountant to recover the loss on the transaction. Accountants who prepared or audited the financial records are attractive targets when the lender or broker's business relationship with the borrower sours because the accountant usually has professional liability insurance coverage whereas the borrower may be judgement proof or bankrupt.

Legal Principles

An accountant's exposure to non-client third-party liability varies from state to state. It is important that accounting professionals are well-versed in identifying this risk and are aware of the legal implications of such requests as they become more common. Privity is generally defined as the connection or relationship existing between two or more contracting parties. Accountants are in privity with their clients because the accountant agrees to provide professional services in return for the client's agreement to pay for those services, thereby creating a contract. The lack of privity is a defense used to bar claims for economic losses in the absence of a contractual relationship between the parties. In the context of professional liability claims, however, the lack of privity defense has eroded and a professional's exposure to liability to third-parties has gained traction in many jurisdictions.

To the extent jurisdictions have taken a position on an accountant's exposure to a third-party, there are essentially five approaches used to evaluate third-party liability. Each jurisdiction has developed its own interpretation of these approaches through case law or enactment of statutes, or a combination of both. Accountants should consult with an attorney to understand how the laws of the jurisdictions where they practice are applied. The five approaches are as follows:

Approach 1: Strict Privity (small minority view)

Some states require actual privity of contract in order to hold an accountant liable for malpractice, so third-parties do not have standing to sue accountants they did not directly engage. In these jurisdictions, the accountant cannot be liable in contract or tort to a third-party in the absence of a written agreement or acknowledgment that the accountant can be held liable by the third-party.

Approach 2: Near Privity

States that follow the "near privity" approach will find an accountant liable to third-parties if the accountant had *actual* knowledge that work product would be used for a particular purpose and the accountant intended that a known third-party would rely on the work product. The third-party must be an intended beneficiary of the engagement by the client of the accountant. For instance, the client hired the accountant to prepare financial statements or opinions specifically for the third-party. Additionally, there must some linking conduct between the accountant and the third-party, such as meetings to discuss the subject transaction, the accountant sending information directly to the third-party, or some other meaningful contact that demonstrates the accountant's understanding that the third-party intended to rely on the work product. For example, under this approach, an accountant receiving a telephone call initiated by the bank that is short and not particularly substantive in nature

Continued on page 7

(ACCOUNTANTS) *Continued from page 5*

would not be sufficient to establish the required linking conduct.

Approach 3: Restatement (2d) of Torts §522 (Majority view)

A majority of jurisdictions follow the approach set forth in Section 522 of the Restatement (2d) of Torts. Under this approach, an accountant's liability is limited to losses incurred by classes of intended users whom the accountant knows will receive and potentially rely on the work product. The first inquiry is whether the person or the class of persons were actually foreseeable or intended users of the information. Then, the court considers whether reliance by the person or class of persons was justifiable. The person or class of persons is foreseeable if the accountant supplies the information directly to the third-party or if the accountant is aware of the client's intent to supply the information to a third-party. In making these inquiries, different jurisdictions may give greater or less weight to different factors and differ in their analysis of various scenarios, but in all instances the Restatement is a somewhat broader approach than the "near privity" approach.

Approach 4: Foreseeability (Minority view)

The broadest approach, which creates greater risk of accountant liability for third-party reliance, is the foreseeability approach. Only a few jurisdictions follow the foreseeability approach. In those states, the accountant may be liable to anyone whose reliance on the professional service was *reasonably* foreseeable (as opposed to the *actually* foreseeable standard under the Restatement (2d) of Torts § 522 approach).

Approach 5: Statutory Approach

Several jurisdictions have statutes that define when an accountant may be liable to a non-client third-party. Although some have enacted the Restatement approach as law, others have statutes with more narrowly drawn requirements specifying when an accountant could be liable to a third-party. In some of these jurisdictions, the accountant can limit exposure to third-parties by sending a notice to the client identifying, and thereby limiting, who is authorized rely on the work product. In one jurisdiction, third-party liability to financial institutions is cut off unless the accountant specifically provides written authorization to the institution agreeing to be held liable to that particular third-party.

Takeaways

Accountants should consult with an attorney or risk management professional to discuss applicable laws, ask questions, and to determine the best of course of action when confronted with these types of requests and the inherent risks they present. Here are some other considerations accounts should bear in mind when asked to verify work-product to non-clients:

- **No good deed goes unpunished.** Being your client's trusted advisor does not mean you need to put yourself in harm's way. The client should get financing or insurance, or achieve whatever desired results, based on the merit of the client's application and not based on the fact that the client has an accountant who responds to questions on the accountant's letterhead. Similarly, the lender, insurer or other relevant third-party must make a business decision based on its analysis of the application and the merit of the transaction, and not based on the fact that the applicant's accountant has professional liability insurance. Accordingly, here

Continued on page 9

Editors' Corner

The Editors are proud to publish this latest edition of *The Defense Line*, which features several interesting articles from our members. We thank the following individuals for their contributions: **Veronica Jackson**, **Robert Wells**, and **Chris Tully** of Miles & Stockbridge, **Maryan Alexander** of Wilson Elser, **Holly Drumheller Butler**, of Miles & Stockbridge, and **Marc Raspanti** of Pietragallo Fordon Alfano Bosick & Raspanti, and **Jeff Trueman**. The Spring is going to be action-packed for the Maryland Defense Counsel. We are wrapping up this legislative session where MDC members are active in sponsoring and fighting bills in Annapolis that affect our community and we have a full schedule of upcoming lunch and learn opportunities and social events. Please visit the Maryland Defense Counsel website (www.mddefenscounsel.org/events) for full information on the organization of upcoming events. We look forward to seeing you!

The Editors sincerely hope that you enjoy this issue of *The Defense Line*. In that regard, if you have any comments or suggestions or would like to submit an article or case spotlight for a future edition of *The Defense Line*, please feel free to contact any member of the Publications Committee, listed below.

Sheryl A. Tirocchi
Chair,
Publications Committee
GodwinTirocchi, LLC
(410) 418-8778

Nicholas J. Phillips
Vice-Chair,
Publications Committee
Gavett, Datt & Barish, P.C.
(301) 948-1177

James K. O'Connor
Vice-Chair,
Publications Committee
Venable
(410) 244-5217

(ACCOUNTANTS) *Continued from page 7*

are some best practices to keep in mind:

— Keep contact with these third-parties to a minimum;

— Do not agree to meetings, calls or direct submissions to third-parties unless there is a compelling business reason to do so and it is made clear in advance that you are only responding to questions based on the limited work performed;

— Always point out in any encounter with a third-party that the services you provided were limited and that the services were not undertaken to influence or replace the third-party's own assessment or judgment;

— Never agree to sign a privity letter or similar acknowledgment;

— Specify in engagement letters and other communications that your services are performed only for the benefit of the client and not for any third-party; and

— Discuss the matter with knowledgeable legal counsel or risk management professionals whenever these issues come up.

- **Know the professional standards.** Accountants should be familiar with applicable professional standards. The professional standards may prohibit certain activity. For instance, the professional standards prohibit an accountant from providing assurance on solvency.
- **Be mindful of confidential information.** Accountants should be cautious of disclosing any confidential client information. Internal Revenue Code 7216 prohibits disclosure of tax information and returns, as well as any information obtained from a taxpayer, unless the taxpayer consents in writing or the disclosure fits within a specified exception under the Code. Confidential information and client communications are further protected by the accountant-client privilege in some jurisdictions and by professional ethics guidance in all situations, so the necessary written waivers must be obtained prior to disclosing such information to third-parties.
- **Control exposure by limiting the scope of the engagement with the client.** Accountants should always review the terms of the engagement with the client and pay close attention to any provisions that create potential exposure for third-party liability. Language referencing reliance by a third-party on the accountant's work product should raise red flags. Accountants should be particularly cautious when asked to verify the information on tax returns to third parties given that the accountant does not independently verify the underlying information provided by the client.

  Accountants should identify the end user of the professional services and the work product at the beginning of each engagement. Accountants can then consider the laws of each jurisdiction that may apply, which may include where the accountant, the client, and the end users are domiciled.

  Accountants can preemptively include language in engagement letters with clients, indicating that they will not respond to any requests for verification from third-parties or that they prohibit the client from sharing the accounting work with third-parties without the accountant's prior consent. Accountants can further mitigate risk by limiting interactions with third-parties to avoid creating a situation where the third-party later claims reliance on those communications.

  If the accountant is aware that certain end users will rely on the work product, the accountant can limit the persons or class of persons to whom the accountant can be liable by sending a letter to the client identifying the persons the accountant is aware will rely on the financial statements. This way the accountant will clearly define to whom he or she may be liable.
- **Responding to verification requests or to notices from third-parties of intended reliance.** In some instances, a third-party will notify the accountant of its intended reliance on the accountant's work product. The accountant should strongly consider sending written notice to the third-party indicating that he/she does not consent to the third-party's reliance and does not agree to be responsible for any action the third-party takes going forward.

Clients often pressure their accountants to help them out with their lender or other third-parties the clients are negotiating with for various reasons. Accountants always want to help their clients, and the pull of the anxious or desperate clients may be hard to resist; however, serving clients well does not mean exposing yourself to liability. Be extremely careful when asked to interact with third-parties or you just might be exposing yourself to risk and potential liability.

Maryan Alexander, a Partner at Wilson Elser, focuses her practice on complex commercial and civil litigation involving financial services, products liability, construction matters, toxic torts and other general casualty claims. She also handles contract negotiations and advises clients on insurance regulatory matters and third-party risk management.

Get Involved With MDC Committees

To volunteer, contact the chairs at

www.mddefensecounsel.org/leadership.html

See photos from past events at mddefensecounsel.org/gallery

Biometric Data: Companies Should Act to Mitigate Risks in the Face of Growing Regulations and Increased Risk for Liability

Chris Tully, Robert Wells, and Veronica Jackson



There is a growing trend to regulate collection and storage of biometric data and severely punish companies who do not adequately protect this data. Every company that collects or uses biometric data must be careful to ensure compliance with applicable laws intended to protect this sensitive information.

What is Biometric Data?

Biometric data is generally defined as "unique physical identifiers including fingerprints, facial structures, iris scans, and voiceprints." While there are no current Federal laws governing the collection, use, and protection of biometric data, several states do specifically regulate this most sensitive information.

It is Much More than HIPAA.

When considering risk related to protecting personal information, we tend to focus on personally identifiable health information protected under HIPAA, or requirements related to protecting sensitive information in the finance industry under the Gramm-Leach-Bliley Act. However, tech-savvy companies in virtually every industry have been using biometric information for years, and increased use and storage of this type of information is gaining in popularity. This increased use is largely because these unique physical identifiers are believed to offer greater security than alphanumeric passwords or other traditional security measures that can be easily faked or stolen.

Companies are recognizing that use of biometric information can be an advantageous business tool, both because of the security protections and as biometric applications create operational efficiencies. Particularly in the health care industry, companies have been quick to broadly embrace the use of biometric identifiers in their operations. For example, large hospital systems in Texas and New York now use palm screening tools for patient intake to streamline administrative processes, avoid patient confusion, and cut down on burdensome paperwork. In addition, health care apps continue to be developed by tech entrepreneurs which track, store, and transmit biometric information to providers for more efficient patient treatment.

The collection, use, and storage of biometric identifiers, however, carries substantial legal risk. Physical attributes that make up biometric information are difficult to replicate and, therefore, offer tremendous value for cybersecurity criminals. In addition, the damage to a consumer caused by theft, leakage, or loss of biometric information is substantial—much more so than a stolen password which can be easily changed. As a result, new laws are being introduced and passed throughout the country to regulate handling of this information, and affected businesses should be vigilant in monitoring statutes, regulations, and proposed legislation, and adjust their policies and procedures accordingly.

Where is Biometric Data Regulated?

Currently, only Illinois, Washington and Texas have statutes specifically devoted to the protection of biometric information. Illinois, in particular, has become a litigation lightning rod for corporations that collect, store, and use biometric information. The Illinois Biometric Information Privacy Act ("BIPA") is unique because it allows for a private cause of action. Early in 2019, risk for liability under the BIPA significantly increased when the Illinois Supreme Court held that plaintiffs are not required to allege actual injury to collect damages, seek injunctive relief, and obtain attorneys' fees under the law. *See Rosenbach v. Six Flags Entertainment Corp.*, 129 N.E.3d 1197 (Ill. 2019). In *Rosenbach*, the Court allowed for damages against Six Flags because it did not provide specific statutory disclosures related to the collection and use of biometric data it obtained from customers, even though the plaintiffs made no assertion that the data had in any way been misappropriated or misused, or that they had incurred any losses. *Id.* at 1207.

Since then, class actions brought under BIPA have dramatically increased. Defendants include technology giants such as Facebook, Google, and Shutterfly, as well as national corporations like The Home Depot, Lowes, and Wendy's. Importantly, a recent challenge involving BIPA in the U.S. Court of Appeals for the Ninth Circuit was unsuccessful, and a unanimous three-judge panel reaffirmed the principle that actual damages are not required for class action certification under BIPA. *See Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019). "[W]e conclude that BIPA protects plaintiffs' concrete privacy interests and violations of the procedures in BIPA actually harm or pose a material risk of harm to those privacy interests." *Id.* at 1275. Accordingly, violations of BIPA are essentially strict liability offenses. The private right of action makes prosecution for violations particularly appealing in the class action context and companies should increase scrutiny of policies and procedures related to biometric data they possess.

While some states, including California, have incorporated biometric information protections into larger consumer protection laws, several other jurisdictions including Arizona, Colorado, Delaware, Georgia, Iowa,

Continued on page 13

(BIOMETRIC DATA) *Continued from page 11*

Louisiana, Massachusetts, Nebraska, New Mexico, New York, Maryland, Massachusetts, Vermont, Wisconsin, Wyoming, and Vermont include biometric information in definitions of protected information for their respective data breach notification laws. In addition, several state legislatures are actively seeking to pass laws specifically related to biometric data privacy and have seen the introduction of related bills in 2019 and 2020 legislative sessions.

The United States Congress also is focusing on this issue with the introduction of SB 847 in 2019, the Commercial Facial Recognition Privacy Act of 2019 ("CFRPA"), which is still being debated but enjoys bipartisan support. CFRPA would prohibit commercial users of facial recognition technology from collecting and re-sharing data for identifying or tracking consumers without the consumer's consent; require companies to notify consumers when facial recognition technology is being used; and require third-party testing and human review of facial recognition technologies prior to their implementation in an effort to address concerns related to inaccuracy and bias that could cause harm to consumers.

As noted above, current and pending laws related to biometric information are complex and vary greatly from state to state. As new legislation continues to be introduced and considered, the risks for companies that collect or use biometric information will continue to increase. In order to ensure compliance with applicable laws while taking advantage of this important and rapidly developing technology, businesses that collect, store, use, or otherwise access biometric information must be aware of all legal requirements and potential for liability, and take steps to implement policies and procedures that, at a minimum, meet any applicable statutory requirements.

For further assistance with biometric privacy laws, including the development and implementation of corresponding policies and procedures, please contact Robert Wells, Michele Cohen, Veronica Jackson or Christopher Tully.

Veronica D. Jackson is a principal at Miles & Stockbridge, P.C. She represents employers in a broad range employment litigation matters, employment discrimination, sexual harassment, ADA and FMLA litigation, and wrongful discharge. Veronica also has extensive experience conducting internal investigations for clients regarding allegations of workplace harassment, discrimination, retaliation under VII and ADA, and regarding incidents related to workplace violence concerns.

Robert Wells is a principal at Miles & Stockbridge. He focuses on healthcare regulatory and corporate matters, representing both long-established and startup healthcare companies. He has advised on a broad array of complex legal and operational matters, including the development and implementation of corporate compliance programs, healthcare commercial acquisitions, employment issues, and regulatory issues.

Christopher Tully is an associate at Miles & Stockbridge. He is a health care lawyer with broad-based transactional, regulatory, and litigation experience. His practice includes representing health care providers and affiliated entities in business and employment contract negotiation, fraud and abuse compliance, state and federal investigations, and certification and accreditation matters.

Upcoming MDC Events

March 10, 2020

Lunch & Learn:
Effective Use of Technology at Trial (ft. UltraDep)

Speakers: Michael G. Miller and Jonathan Huber, Esq.
Miles & Stockbridge (Baltimore)
12:00 pm – 1:00 pm

MGM TRIAL SERVICES, INC.

March 27, 2020

MDC Happy Hour

Mt. Washington Tavern
5700 Newbury Street
Baltimore, Maryland 21209
6:00 pm – 8:00 pm

Exponent®

April 24, 2020

Lunch & Learn:
Advocacy in Mediation

Speaker: Hon. Martin P. Welch
Miles & Stockbridge (Baltimore)
12:00 pm – 1:00 pm

Approved for 1.0 credit hours for Virginia CLE credit

THE McCAMMON GROUP

May 15, 2020

Lunch & Learn

Speaker: Christina Billiet, Esq.
Location: Miles & Stockbridge (Baltimore)
Time: 12:00 pm – 1:00 pm

ION MEDICAL DESIGNS

Tips For Representing Cos., Employees In Gov't Investigations

Holly Drumheller Butler and Marc Raspanti

Individual liability continues to be at the forefront of criminal investigations and the litigation that often follows. Throughout the past five years, the U.S. Department of Justice's edicts on individual culpability have varied in tone and rigidity, but the underlying focus on individuals has remained constant.

On Sept. 9, 2015, former Deputy Attorney General Sally Yates authored a memorandum on corporate prosecution, now referred to as the "Yates memo.[1] The Yates memo, which memorialized the DOJ's long-standing policy that individual accountability is one of the most effective ways to deter corporate crime, recommended an all-or-nothing approach that sent shock waves through the legal community, who feared that cooperation credit had been rendered an unattainable fiction.

On Sept. 25, 2018, the DOJ updated the U.S. Attorney's Manual to include a modified version of the Yates Memo, requiring corporations to "identify all individuals substantially involved in or responsible for the misconduct at issue" to obtain consideration for cooperation credit.[2]

Subsequently, DOJ leadership has reiterated its focus on individual liability. As recently as last month, Deputy Assistant Attorney General Matthew Miner delivered remarks at the Sixth Annual Government Enforcement Institute in which he highlighted that the DOJ remains "focused on investigating and prosecuting the individuals responsible for fraudulent behavior and corporate crime."[3]

To underscore his point, he referenced the DOJ fraud section's recent prosecution numbers, noting that in 2018, that section alone prosecuted 422 individuals, representing an almost 37% increase from the prior year.[4] Indeed, this focus on individual prosecutions was emphasized emphatically several weeks later, on Sept. 27, when the DOJ filed charges against 53 individuals in a health care fraud law enforcement action and 35 individuals in a fraudulent genetic testing ring in one of the largest health care fraud schemes ever charged.[5]

However, the U.S. government is not the only one who recognizes the impact of individually named defendants. Qui tam relators and their private counsel are initiating a majority of the litigation stemming from whistleblower complaints, particularly in the healthcare field. Relators are naming individuals, private equity firms, corporations, and even competitors at an unprecedented rate.

As a result, the corporate client may be in conflict — current or future — with its executives or employees whom the government, relator, or the corporation itself, has identified as engaging in the misconduct. On a bad day, that conflict could lead to disclosure of client confidences or disqualification of both sets of outside defense counsel. One needs to look no further than U.S. v. Weissman to understand the adverse implications of counsel concurrently representing the corporation and potentially targeted executives in connection with a government investigation.[6]

To avoid this unfortunate result, investigations of corporations and its executives or employees require attentiveness to who is the "client" much sooner rather than later and should adhere to the following best practices:

Corporation vs. Individuals

Defense counsel who are hired to represent a company do not represent the individual employees. This is the reason a chilling "Upjohn" warning must be given to every executive or individual employee before any interview is conducted of them. At the outset of an investigation, corporate counsel usually does not have a robust picture of where the government investigation is going or which individuals may be involved or implicated. Therein lies the relevant conflict issue.

The prudent course is to suggest, or even insist, that potentially impacted employees retain competent independent counsel before any meaningful interviews begin. Corporate counsel should resist the temptation to exercise sole control and envelope everything within their reach. The temporary gains obtained in information and control can all be jeopardized if and when a conflict arises

Clients Must Choose Defense Counsel Wisely

Government investigations are becoming more, not less, complex. They are multifaceted and often highly coordinated. A typical investigation often includes state, federal and regulatory authorities. Individual targets, subjects or even witnesses who become embroiled in an investigation must choose their defense counsel carefully. Relevant experience in the subject matter is an important requisite to retention. More importantly, the ability to sort through an ever changing landscape of government enforcement personnel, co-defendants and their counsel, and even qui tam relators and their counsel is necessary.

Joint Defense and Common Interest Agreements

Joint defense and common interest agreements enable the parties to work together to investigate the facts, while preserving each party's defenses, privileges, confidences, and protections — so long as a common interest exists. The common interest doctrine, which is an extension of the attorney-client privi-

Continued on page 15

[1] https://www.justice.gov/archives/dag/file/769036/download

[2] https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations#9-¬ 28.700

[3] https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-matthew-s-miner-delivers-¬remarks-6th-annual-government

[4] *Id.*

[5] https://www.justice.gov/opa/pr/midwest-health-care-fraud-law-enforcement-action-results-¬charges-against-53-individuals (Midwest Health Care Fraud Law Enforcement Action Results in Charges Against 53 Individuals Alleging $250 Million in Loss); https://www.justice.gov/opa/pr/federal-law-¬enforcement-action-involving-fraudulent-genetic-testing-results-charges-against (Federal Law Enforcement Action Involving Fraudulent Genetic Testing Results in Charges Against 35 Individuals Responsible for Over $2.1 Billion in Losses in One of the Largest Health Care Fraud Schemes Ever Charged).

[6] *U.S. v. Weissman*, 1996 WL 737042 (SDNY Dec. 26, 1996 (involving corporate counsel representing both the company and CFO at initial stages of investigation and in course of witness interviews with government investigators prior to CFO seeking separate representation, resulting in disclosure of arguably privileged memoranda).

(GOV'T INVESTIGATIONS) *Continued from page 14*

lege, applies even where there is no litigation in progress.

Thus, in most circumstances the doctrine can apply in the context of a corporate entity's internal investigation of potential wrongdoing, whether or not the government is already involved or a whistleblower has made a claim. While the timing of the communications (e.g., before litigation is initiated or reasonably anticipated) is not controlling for the doctrine to apply, the substance is; only those communications made in connection with and in furtherance of the common enterprise are privileged.

While the joint defense arrangement is in place, counsel for the corporation and counsel for the employees or executives should share relevant facts and information. The government will have a full picture of the underlying issues and potential defenses from its broad document review and compelled witness interviews. Corporations and individuals should endeavor to be on even footing and to have the same fulsome understanding of the facts or the representation will be in jeopardy.

Reevaluate Potential Conflicts Between the Corporation and Individuals

Although joint defense arrangements can be mutually beneficial, factual developments and various strategic decisions can impact the continuation of that arrangement. For example, an individual's or corporation's decision to cooperate with the government in an investigation may impact joint defense. Individuals and corporate entities have different considerations for determining whether to cooperate in a government investigation.

If an employee or executive is facing personal criminal exposure, that individual can obtain benefits from early and complete cooperation with the government. Such cooperation benefits run the spectrum from nonprosecution agreements or deferred prosecution agreements to reduced sentences/financial penalties to immunity for the criminal conduct the government has charged or may charge.

To obtain such relief, the government may require cooperative assistance — including participation on investigative operations, such as recording telephone calls or wearing a wire to in-person meetings under an agent's supervision — that is at odds with the interests and legal defenses of the corporation.

Conversely, for a corporation to be eligible for cooperation credit, the entity must provide the DOJ with all relevant facts related to the misconduct and identify of all individuals substantially involved in or responsible for the misconduct.[7] If a corporation is brought into the investigation following a grand jury indictment or guilty plea of an executive, the entity may have a compulsion to cooperate and identify any additional wrongdoings for its own protection and preservation. This may create untenable conflicts if individuals and the company are represented by the same counsel.

Potential Insurance Coverage

As a final note, whether representing the corporation or, just as importantly, an employee, all relevant insurers should be notified immediately of a government investigation if it could potentially be considered a claim. Unfortunately, too many seasoned practitioners ignore this important step at significant peril to the client.

Corporations and individuals should err on the side of caution in determining whether to notify the insurer of a potential claim emanating from a government investigation. Although coverage will vary depending on the definitions of the "claim" and the "insured," prompt written notice, containing a plain statement of the claim, should be provided to the carrier to avoid a denial of coverage for lack of timely notice.

As government investigations and qui tam litigation continue to focus on allegations of individual's misconduct, it is imperative to be cognizant of the risks and emerging best practices associated with the legal representation of those employees and their current or former employer. Strategic and privilege considerations are not static and must be reevaluated and revisited throughout the investigation as facts develop.

Holly Drumheller Butler is a principal at Miles & Stockbridge PC.

Marc S. Raspanti is a name partner of Pietragallo Gordon Alfano Bosick & Raspanti LLP.

Note: This article appeared previously at www.mslaw.com on October 30, 2019 and on Law360.

[7] See infra fn. 2.

"This is Mediation so it's Confidential, Right?" Confidentiality Tips When Mediating Disputes In and Out of Maryland State Courts

Jeff Trueman

The Maryland Court of Appeals adopted new standards of conduct for court-appointed and non-court-appointed mediators, effective Jan. 1, 2020. The standards of conduct (available at https://www.courts.state.md.us/sites/default/files/import/macro/pdfs/mdstandardsofconductformediators.pdf), the Title 17 of Maryland Rules, and the Maryland Confidentiality Act (Md. Code, Courts and Judicial Proceedings, section 3-1801, et. seq., referred to here as the Maryland Confidentiality Act) play a role in determining whether your mediation communications are confidential. As explained in this article, participants should not expect a vague sense that "the law" or the Maryland Rules will automatically protect mediation communications. Instead, in my opinion, participants should execute a confidentiality agreement to best protect mediation communications.

Recall that confidentiality in mediation is protected under the Maryland Rules only in court-referred cases. See Md. Rule 17-101(a) and 17-105. Even then, it only applies to mediation as it is defined under Md. Rule 17-102(g) ("'Mediation' means a process in which the parties work with one or more impartial mediators who, without providing legal advice, assist the parties in reaching their own voluntary agreement for the resolution of all or part of a dispute.") and Md. Rule 17-103. ("While acting as a mediator, the mediator does not engage in any other ADR process and does not recommend the terms of an agreement."). These definitions do not reflect what most attorneys and claims professionals experience in private, commercial mediations.

Settlement conference practitioners do not labor under such restrictions. *See* Md. Rule 17-102(l) ("'Settlement conference' means a conference at which the parties, their attorneys, or both appear before an impartial individual to discuss the issues and positions of the parties in an attempt to agree on a resolution of all or part of the dispute by means other than trial. A settlement conference may include neutral case evaluation and neutral fact-finding, and the impartial individual may recommend the terms of an agreement."). Although settlement conference neutrals have more leeway to employ techniques that will resolve legal disputes, surprisingly, they are afforded no confidentiality protections under the Maryland Rules or the Maryland Confidentiality Act. Similarly, there is **no** confidentiality protection for neutral evaluation and fact-finding.

The Maryland Confidentiality Act protects communications made in mediations that occur outside of a court order but **only** if the mediator states **in writing** that he or she will adhere to the new standards. See Md. Code, Courts and Judicial Proceedings, Section 3-1802(a)(3). As far as I know, many if not most commercial mediators do not state in writing that they will follow the new standards. I suspect many are unaware of this requirement. Some may choose to opt out of the standards for the following reasons.

There is a long-standing power-struggle for the heart and soul of mediation in Maryland. At the heart of the dispute is whether evaluative mediation is legitimate. In my view, the judiciary's view of mediation is narrower and more conservative than what we practice in private, commercial mediation. This is why the Maryland Rules define "settlement conference" differently than "mediation." The problem is that settlement conferences on paper resemble what most everyone else (litigators, claims professionals, institutional representatives, and commercial mediators) experience when privately mediating litigated disputes.

To make a very long story short, we now have disparate standards of what the judiciary says mediation is on paper and what is practiced each and every day in conference rooms across the state. This is a reflection of disparate values within Maryland's dispute resolution community. For the most part, the private marketplace values resolution and settled cases. In my view, the judiciary does not; it advises mediators to resist "pressure" to settle cases (see page 6 of the new standards; https://www.courts.state.md.us/sites/default/files/import/macro/pdfs/mdstandardsofconductformediators.pdf). The private marketplace values the self-determination of parties who wish to engage in evaluative mediation. In my view, the judiciary does not; it demotes self-determination when it comes to evaluative mediation (page 5, Drafters Notes 5 & 6 of the new standards; https://www.courts.state.md.us/sites/default/files/import/macro/pdfs/mdstandardsofcon-

Continued on page 19

The MDC Expert List

The MDC expert list is designed to be used as a contact list for informational purposes only. It provides names of experts sorted by area of expertise with corresponding contact names and email addresses of MDC members who have information about each expert as a result of experience with the expert either as a proponent or as an opponent of the expert in litigation. A member seeking information about an expert will be required to contact the listed MDC member(s) for details. The fact that an expert's name appears on the list is not an endorsement or an indictment of that expert by MDC; it simply means that the listed MDC members may have useful information about that expert. MDC takes no position with regard to the licensure, qualifications, or suitability of any expert on the list.

To check out the **MDC Expert List**, visit **www.mddefensecounsel.org** and click the red "Expert List" button in the left hand corner of the home page or access it from the directory menu.

MINNESOTA LAWYERS MUTUAL'S

Defense Program

INSURANCE SPECIFICALLY DESIGNED AND RATED FOR DEFENSE FIRMS

Members of the Maryland Defense Counsel, Inc. have access to MLM's Defense Program – offering a lawyers' professional liability policy with preferred pricing and enhanced coverage.

Two Ways to Save

- **Preferred pricing** for firms with substantial insurance defense practice
- **A 5% membership credit -** Credit applied to premium on a per attorney basis

Enhanced Coverage*

- **Additional Claim Expense -** Benefit equal to one-half of the policy single limit, up to a maximum of $250k per policy period
- **Increased Supplementary Payment Limit -** From $10k to $25k - this includes loss of earnings if you attend a trial at our request and coverage for costs and fees incurred defending disciplinary claims
- **Aggregate Deductible -** Caps the total amount the insured will have to pay in total deductibles regardless of the number of claims in a single policy period

*Visit **www.mlmins.com** for qualification details

"We are proud to offer coverage to MDC membership. MLM has long been recognized as a financially stable and consistent carrier for Maryland lawyers, and we're thrilled to benefit members of the association."

Paul Ablan, President and CEO
Minnesota Lawyers Mutual

Protect your firm with the ***premium savings*** and ***enhanced coverage*** offered to you as a member of the Maryland Defense Counsel, Inc.

Apply for a quote online!

www.mlmins.com

DEFENSE PROGRAM
MINNESOTA LAWYERS MUTUAL
INSURANCE COMPANY

Contact
Kiernan Waters, Esq.
Regional Sales Director
Cell: 433.293.6038
kwaters@mlmins.com

Spotlight

Nikki Nesbitt Named 2020 Chair of The Network of Trial Law Firms

Goodell DeVries is pleased to announce that **Nikki Nesbitt** has been named Chair of The Network of Trial Law Firms for 2020. Nikki has served on the Network's Executive Committee since 2017 and previously held the roles of Secretary, Treasurer and Vice Chair. She has also served as a Seminar Chair and presented at Network events on a variety of topics.

Founded in 1993, The Network of Trial Law Firms, Inc. remains committed to the art of strengthening strategic business relationships amongst the country's leading trial law firms. Its mission is to connect the world's leading corporations with world-class legal experts. The Network includes over 5,000 attorneys in 24 separate and independent trial law firms practicing in over 120 offices throughout the United States.

Nikki is a partner in Goodell DeVries and focuses her practice on medical malpractice defense and complex commercial litigation, as well as cases that combine the two fields. For the entirety of her 18 years at the bar, Nikki has practiced at Goodell DeVries and has moved through the ranks from summer associate to partner. She has also served in leadership positions in the Maryland Defense Counsel, the Defense Research Institute, and in non-legal organizations such as JDRF.

(MEDIATION) *Continued from page 17*

ductformediators.pdf) – a process not recognized by the "Mediator Excellence Council" (see page 4 of the Maryland Program for Mediator Excellence, Mediation Framework Descriptions; https://www.courts.state.md.us/sites/default/files/import/macro/pdfs/mpmemediationdefinitions.pdf).

It seems clear to me that the drafters of the Maryland Rules and the new standards wanted to prioritize and incentivize adherence to their form of mediation above all other dispute resolution processes. Apparently, confidentiality was supposed to be the carrot.

Although the Maryland Rules of Evidence make most settlement discussions inadmissible (Md. Rule 5-408(a)), one state case found the Rules of Evidence inapplicable since the parties were fighting over whether they had, in fact, reached a deal as opposed to the "validity, invalidity, or amount of a civil claim[.]" *Sang Ho Na v. Gillespie*, 234 Md. App. 742, 751 (2017) (quoting Md. Rule 5-408(a)). Settlement discussions can also be admitted under Md. Rule 5-408(c) "when offered for another purpose, such as proving bias or prejudice of a witness, controverting a defense of laches or limitations, establishing the existence of a 'Mary Carter' agreement, or by proving an effort to obstruct a criminal investigation or prosecution." Thus, the Rules of Evidence may offer some protection but perhaps not as much as Title 17 of the Maryland Rules of the Maryland Confidentiality Act.

Consequently, in my opinion, your mediator should have all participants sign a confidentiality agreement that applies no matter what process you use. As you now know, not all "mediations" are the same. "The law" may not intrinsically protect your communications just because you engage in a process you think is mediation. If the Maryland Rules apply to your case because of a court order to mediate, perhaps you can engage a mediator of your choosing without the court's permission in order to get around Title 17's narrow view of mediation. If the case does not settle, however, the court's order to mediate still stands. Thus the best practice might be to opt out of every order to mediate within 30 days of its issuance so that parties retain control over the process. As mentioned, the Rules of Evidence may not provide enough protection. The durability of a confidentiality agreement may be tested, but it should clearly indicate an intention by all participants to keep mediation communications confidential. *See Sang Ho Na*, 234 Md. App. at 751-52. In my opinion, a well-worded agreement, unlike that in the *Sang Ho Na* case, will outline a process to resolve subsequent disagreements over performance of the settlement terms, eliminating the need for court enforcement.

See photos from past events at mddefensecounsel.org/gallery

The author is a private commercial mediator in Baltimore and the past director of Civil ADR for the Circuit Court for Baltimore City. He can be contacted at jt@jefftrueman.com.

Official Sponsors

Courthouse Copy
Paper-Images-Online

The Daily Record

Gold Sponsors

Exponent®

The McCammon Group

Defense Program
Minnesota Lawyers Mutual

Rimkus
Consulting Group, Inc.

Veritext
Legal Solutions

Silver Sponsors

Planet Depos
We Make It Happen™

S-E-A

Bronze Sponsors

ION
Medical Designs

MGM
Trial Services, Inc.

The National Academy of Distinguished Neutrals
Maryland Chapter

Sustaining Members

Miles & Stockbridge

WTP Whiteford | Taylor | Preston LLP