Consumer Law Meets Cyber Law:

Emerging Consumer Protection Issues in Light of Digital Innovation and Technology Advancements

2020 Virtual
Florida Bar Annual Convention
Friday, June 19, 2020, 1 p.m. – 5 p.m.

Intermediate Level
Course No. 3363
CLE Credits: General: 4 Technology: 4

A Presidential Showcase Seminar
Presented by the

Consumer Protection Law Committee

Common Questions About CLER

1. What is CLER?
CLER, or Continuing Legal Education Requirement, was adopted by the Supreme Court of Florida in 1988 and requires all members of The Florida Bar to continue their legal education.

2. What is the requirement?
Over a three-year period, each member must complete 33 hours, 5 of which are in the area of ethics, professionalism, substance abuse, or mental illness awareness, and 3 hours in technology.

3. Where may I find information on CLER?
Rule 6-10 of the Rules Regulating The Florida Bar sets out the requirement. All the rules may be found at www.floridabar.org/rules.

4. Who administers the CLER program?
Day-to-day administration is the responsibility of the Legal Specialization and Education Department of The Florida Bar. The program is directly supervised by the Board of Legal Specialization and Education (BLSE) and all policy decisions must ultimately be approved by the Board of Governors.

5. How often and by when do I need to report compliance?
Members are required to report CLE hours earned every three years. Each member is assigned a three-year reporting cycle. You may find your reporting date by logging in to your member portal at member.floridabar.org.

6. Will I receive notice advising me that my reporting period is upcoming?
Four months prior to the end of your reporting cycle, you will receive a CLER Reporting Affidavit, if you still lack hours.

7. What happens if I am late or do not complete the required hours?
You run the risk of being deemed a delinquent member which prohibits you from engaging in the practice of Florida law.

8. Will I receive any other information about my reporting cycle?
Yes, you will receive reminders prior to the end of your reporting cycle, if you have not yet completed your hours.

9. Are there any exemptions from CLER?
Rule 6-10.3(c) lists all valid exemptions. They are:
1) Active military service
2) Undue hardship (upon approval by the BLSE)
3) Nonresident membership (see rule for details)
4) Full-time federal judiciary
5) Justices of the Supreme Court of Florida and judges of district, circuit and county courts
6) Inactive members of The Florida Bar

10. Other than attending approved CLE courses, how may I earn credit hours?
Credit may be earned by:
1) Lecturing at an approved CLE program
2) Serving as a workshop leader or panel member
3) Writing and publishing in a professional publication or journal

4) Teaching (graduate law or law school courses)
5) University attendance (graduate law or law school courses)

11. How do I submit various activities for credit evaluation?
Applications for credit may be found on our website, www.floridabar.org.

12. How are attendance hours posted on my CLER record?
You must post your credits online by logging in to your member portal at member.floridabar.org.

13. How long does it take for hours to be posted to my CLER record?
When you post your CLE credit online, your record will be automatically updated, and you will be able to see your current CLE hours and reporting period.

14. How may I find information on programs sponsored by The Florida Bar?
You may wish to visit our website, www.floridabar.org/cle or refer to The Florida Bar News. You may also call CLE Registrations at 850/561-5831.

15. If I accumulate more than 30 hours, may I use the excess for my next reporting cycle?
Excess hours may not be carried forward. The standing policies of the BLSE, as approved by the Supreme Court of Florida specifically state in 6.03(b):
. . . . CLER credit may not be counted for more than one reporting period and may not be carried forward to subsequent reporting periods.

16. Will out-of-state CLE hours count toward CLER?
Courses approved by other state bars are generally acceptable for use toward satisfying CLER.

17. If I have questions, whom do I call?
You may call the Legal Specialization and Education Department of The Florida Bar at 850/561-5842.

While online checking your CLER, don't forget to check your Basic Skills Course Requirement status.

THE FLORIDA BAR

PREFACE

The course materials in this booklet were prepared for use by the registrants attending our Continuing Legal Education course during the lectures and later in their offices.

The Florida Bar is indebted to the members of the Steering Committee, the lecturers and authors for their donations of time and talent but does not have an official view of their work products.

CLER CREDIT

(Maximum 7 hours)

General . . . . . .4.0 hours
Technology . . .4.0 hours

Seminar credit may be applied to satisfy both CLER and Board Certification requirements in the amounts specified above, not to exceed the maximum credit. Refer to Chapter 6, Rules Regulating The Florida Bar, see the CLE link at www.floridabar.org for more information about the CLER and Certification Requirements.

Prior to your CLER reporting date you will be sent a Reporting Affidavit (must be returned by your CLER reporting date). You are encouraged to maintain records of your CLE hours.

CLE CREDIT IS NOT AWARDED FOR THE PURCHASE OF THE COURSE BOOK ONLY.

CLE COMMITTEE MISSION STATEMENT

The mission of the Continuing Legal Education Committee is to assist the members of The Florida Bar in their continuing legal education and to facilitate the production and delivery of quality CLE programs and publications for the benefit of Bar members in coordination with the sections, committees and staff of The Florida Bar and others who participate in the CLE process.

COURSE CLASSIFICATION

The Steering Committee for this course has determined its content to be:

INTERMEDIATE.

CONSUMER PROTECTION LAW COMMITTEE

Lisa DiFranza — Chair
Victoria Butler — Vice Chair
Charles Geitner — Vice Chair
Anthony Palermo — Vice Chair

CONSUMER PROTECTION LAW COMMITTEE
CLE SUBCOMMITTEE

Jennifer Newton – CLE Co-Chair
Judge Sarah Shullman — CLE Co-Chair
With
Anthony Palermo, Committee Vice Chair
Ruth Jackson Lee
Jared Levy
Derek Mountford
Robert Murphy

FLORIDA BAR
CLE COMMITTEE

Elaine Laverne Thompson — Chair
Terry L. Hill — Director, Programs Division

For a complete list of Member Services, please visit our web site at www.floridabar.org.

OVERVIEW

Digital innovation and technological advancements are changing the way that consumers interact with businesses. Consumers increasingly rely on technology for convenience and simplicity, while companies use new technologies to learn more about customers' wants and needs.

As consumers become more reliant on new technologies, what are the implications for consumer protection and data analytics?

This year's Consumer Protection Law Committee Presidential Showcase CLE focuses on relevant consumer protection issues facing both consumer lawyers and general practitioners. Panelists include successful veterans in the fields of **consumer protection**, **cybercrime**, **data hostage negotiations**, **bitcoin** and **digital currency**, and **data analytics.** Participants will also learn about emerging consumer protection issues including litigation and enforcement trends and ethical and policy implications.

LECTURE PROGRAM

1: p.m.
Introduction and Overview
Lisa Anne DiFranza, Chair, Consumer Protection Law Committee

1:10 p.m. – 2 p.m.
Emerging Consumer Protection Issues
in Light of Innovation and Technology
Advancements
Moderator: **Judge Sarah Shullman, CLE Subcommittee Co-chair**
Speakers:

- Victoria Butler, Division Director, Florida Office of
- the Attorney General
- Lynn Drysdale, Jacksonville Area Legal Aid
- Richard Lawson, Gardner Brewer Martinez-Monfort
- Jared Lee, Jackson Lee
- Alice Vickers, Florida Alliance for Consumer Protection

2 p.m. - 2:10 p.m. BREAK

2:10 p.m. – 3 p.m.
Data Privacy & Security Trends, Data Hostage Negotiations,
& Cybercrime
Moderator: Anthony Palermo, Holland & Knight, Tampa
Speakers:

- Robert Shimberg, Hill Ward Henderson
- Mark Melodia, Holland & Knight LLP (New York), Chair of Data Strategy,
- Security & Privacy Team
- Kevin Rosen, Managing Attorney, Rosen Protection Law PLLC
- G.C. Murray, Managing Member, Association GC

3 p.m. - 3:10 p.m. BREAK

3:10 p.m. - 4 p.m.
Cryptocurrency and Blockchain: Digital Currencies and Smart Contracts
Moderator: Ryan McGee, Morgan & Morgan
Speakers:

- Josias "Joe" Dewey, Holland & Knight LLP (Miami), Chair of Blockchain
- Technology Team
- Shawn Bayern, Professor, Florida State University
- Jordan Maglich, Quarles & Brady, Tampa

4 p.m. - 4:10 p.m. BREAK

4:10 p.m. - 5 p.m.
Machine Learning, Online Data Aggregators and Use of Data Analytics in Litigation
Moderator: Jennifer Newton, Greenberg Traurig, P.A.
Speakers:

- David Dalva, Aon Cyber Solutions
- Tanja Gromadzki, Ethics & Compliance, Tech Data Corporation
- Alfred John Saikali, Florida Bar - Technology Committee, Chair; Shook
- Hardy & Bacon's Privacy and Data Security Practice

TABLE OF CONTENTS

Chapter 1

Chapter 2

Data Privacy & Security Trends, Data Hostage Negotiations, & Cybercrime

LECTURERS

Shawn Bayern's research at Florida State University College of Law focuses on common-law issues, primarily in contracts, torts and organizational law. He has recently written articles criticizing formalism and economic simplifications of the law. He teaches Torts, Contracts, Agency & Partnership and other related courses. Before joining FSU Law, Professor Bayern was a visiting assistant professor at Duke Law School. He has also served as a law clerk for the Hon. Harris Hartz of the U.S. Court of Appeals for the Tenth Circuit, for the Office of the Solicitor General, and at the appellate staff of the Civil Division of the U.S. Department of Justice. He is an elected member of the American Law Institute.

Victoria Butler, director of the Consumer Protection Division at the Florida Attorney General's Office, oversees the state's consumer protection enforcement actions. She has participated in numerous multistate and joint federal/state cases involving business practices such as advertising, telemarketing, robocalling, data security, privacy, financial practices and mortgage servicing. Previously, she was a U.S. District Court law clerk in the Middle District of Florida and served as deputy court counsel to the chief judge in Florida's 13th Judicial Circuit Court. Butler is the recipient of numerous awards, including the U.S. Attorney General's Distinguished Service Award for 2012 and The Florida Bar Consumer Protection Lawyer of the Year Award in 2012. She is a grader for the Florida Board of Bar Examiners and author of the Florida Section of the ABA Consumer Law manual.

David Dalva is vice president of Stroz Friedberg/Aon Cyber Solutions, helping clients proactively manage information and cyber risk. Dalva chaired the NIST Smart Grid Interoperability Panel's Cyber Security Working Group, where he co-led publication and implementation of "Guidelines for Smart Grid Cyber Security" and the Department of Energy's "Electricity Subsector Cybersecurity Risk Management Process" guideline. Dalva began his career in cybersecurity research at Trusted Information Systems, where he was involved in military-funded research on multi-level secure operating systems, cryptographic policy. He was an original designer and developer of one of the first firewall technologies in the market – the Gauntlet firewall, based on the TIS Firewall Toolkit.

Lisa DiFranza, chair of the Consumer Protection Law Committee, focuses her practice on elder law, guardian advocacy, guardianships, probate, and estate planning. In 2018, she was awarded as the Small Business Leader of the Year, Beaches Division, of the JAX Chamber. DiFranza started her solo practice in the area of guardianships and guardian advocacy by volunteering with Jacksonville Area Legal Aid and continues to serve as their practice support for pro bono attorneys and clients. DiFranza enjoys educating colleagues and the public by giving lectures on guardianships, advanced directives, durable powers of attorneys, trusts, advanced directives and probate issues to community and professional groups. She serves on the Jacksonville Bar Association Pro Bono Committee and 4th Circuit Pro Bono Committee, Estate Planning and Tax Committee, and Elder Law Committee.

Josias "Joe" N. Dewey is a partner in Holland & Knight LLP's Miami office. He is a financial services and real estate attorney and is considered a thought leader on blockchain and distributed ledger technology (DLT). Dewey is co-author of the book, "The Blockchain: A Guide for Legal and Business Professionals," published by Thomson Reuters. Dewey formerly served as the leader of Holland & Knight's Miami Real Estate practice group. He is also an experienced software developer, who has created workflow applications to speed up the lifecycle of financing and other transactions. Dewey is an adjunct professor of law at the University of Miami School of Law, teaching a real estate transactions course.

Lynn Drysdale is division chief of the Consumer Litigation and Legislative Advocacy Unit at Jacksonville Area Legal Aid. Drysdale has long been an ally to those who have been abused by unjust lending practices that set borrowers up for failure. Although she primarily represents low-income people, Drysdale has a special interest in older consumers and enlisted and retired members of the armed services and their dependents. She has testified on their behalf in front of legislative bodies. Drysdale has contributed to many consumer law treatises as well as teaching attorneys and "soon to be" attorneys for decades. She has worked to combat deceptive products such as payday loans and illegal loan collection and mortgage servicing, especially with reverse mortgages.

Tanja Gromadzki is the Compliance Specialist for the Americas at Tech Data Corporation. In her role, she leads the implementation of various aspects of the company's compliance program in the Americas, including proactive initiatives, third-party review, and internal investigations support. Her role also focuses on data analytics reporting and benchmarking to help ensure program effectiveness through the developing and monitoring key metrics and effectiveness indicators. Gromadzki has experience working in multi-national operations and is fluent in German. She is a Certified Compliance & Ethics Professional through the Society of Corporate Compliance and Ethics.

Richard Lawson is a partner with the Tampa law firm of Gardner Brewer Martinez-Monfort, where he handles complex commercial litigation and government regulatory investigations. Before joining Gardner Brewer Martinez-Monfort, Lawson served as the director of the Consumer Protection Division for the Florida Attorney General's Office. Lawson received his B.A. from the University of Florida and his J.D. from the Florida State University College of Law.

Jared M. Lee teaches Consumer Protection Law as an adjunct professor at Florida State University College of Law, his alma mater, where he graduated from with honors in 2007. He spent nearly a decade at Morgan & Morgan in the consumer protection department before becoming the managing partner of Jackson Lee PA, where he focuses on consumer-related litigation in both state and federal court. Lee served as a chair of The Florida Bar's Consumer Protection Committee and is currently a state co-chair for Florida with the National Association of Consumer Advocates. He's also appeared on radio and television broadcasts as a specialist in consumer issues.

Jordan Maglich, a member of the Litigation and Dispute Resolution Practice Group in the Tampa office of Quarles & Brady, focuses his practice on commercial litigation, securities and financial services, and regulatory matters. Maglich practices in arbitration forums and state, federal and bankruptcy courts in civil disputes and other business-related litigation. He also represents securities broker/dealers and investment advisers in federal and state court and in arbitration. Maglich counsels and defends individuals and entities facing regulatory inquiries, subpoenas and investigations by state and federal agencies. Recent experience includes identifying, seizing and liquidating various cryptocurrency assets. Maglich also is the author of in the internet blog Ponzitracker.

Ryan McGee works with Morgan & Morgan's Complex Litigation Group in Tampa, where he represents consumers in class action litigation, with a focus on data security, deceptive and unfair practices, and consumer protection. Before that, McGee represented businesses in state and federal courts across the nation. After law school, McGee was appointed a state prosecutor in Pinellas and Pasco counties, where he tried more than 50 jury trials to verdict, including homicides and white-collar crimes. After leaving that post, McGee served as a law clerk for two years for the Hon. Elizabeth A. Kovachevich, a former chief U.S. District judge in Tampa.

Mark Melodia is a privacy, data security and consumer class action defense lawyer in Holland & Knight's New York office and serves as the head of the firm's Data Strategy, Security & Privacy Team. Melodia focuses on governmental and internal investigations, putative class actions and other "bet-the-company" suits in data security/privacy, mortgage/financial services and other complex business litigation, including defamation. Melodia has defended more than 90 putative class actions, including as lead defense counsel in multiple multidistrict litigations arising from alleged consumer privacy violations, data incidents and allegations of data misuse.

G.C. Murray II is the managing member of Association GC, one of the premier association management companies in Florida. Murray is nationally recognized for his legal acumen and his philanthropy. His work focuses on all aspects of nonprofit management, including federal and state compliance, organizational leadership, and high-level fundraising. He is an experienced lobbyist and has worked on issues dealing with the intersection between consumer law, privacy and technology.

Jennifer Newton is an attorney in the Miami office of Greenberg Traurig, P.A., where she is a member of the Corporate and Financial Regulatory Practice Group. She regularly advises banking and financial institutions on risk management and compliance matters relating to federal and state consumer protection laws and regulations. Prior to joining Greenberg, Newton worked as a federal financial services regulator with the U.S. Consumer Financial Protection Bureau.

Anthony J. Palermo is an associate at Holland & Knight LLP in Tampa, where he represents clients in commercial litigation and consumer protection matters and advises on regulatory compliance issues. He has represented multiple professional sports teams in Florida, including Major League Baseball and National Hockey League franchises in business disputes. As part of his regulatory practice, he has been appointed a Special Assistant Attorney General to advise a state-run lending institution on compliance with consumer protection and banking laws. A vice chair of The Florida Bar's Consumer Protection Law Committee, Palermo has authored articles for multiple legal publications. His published work has been cited in law review articles and in a recent decision by Florida's Second District Court of Appeal. He earned his J.D. from Harvard Law School.

Kevin D. Rosen is managing attorney of Rosen Protection Law PLLC in Boca Raton. He assists clients with managing cyber security risk, cyber fraud prevention, security and risk assessments, digital forensics investigations, and incident response and recovery. He has more than 20 years of career experience at the Financial Industry Regulatory Authority, Deloitte Risk & Financial Advisory, the Florida Department of Banking and Finance, and large law firm practice. At FINRA, Rosen focused on investigations, examinations, and prosecutions related to cyber security, privacy, anti-money laundering compliance, and fraud. He is a Certified Information Privacy Professional with the IAPP and a Certified Regulatory Compliance Specialist with the FINRA Institute-Wharton School of Business.

Al Saikali chairs the Privacy and Data Security Practice at Shook, Hardy & Bacon from the firm's Miami office. In that role, Saikali directs breach response efforts for clients, represents companies in privacy and data security litigation, and counsels organizations to help them comply with laws governing the collection, storage, and use of sensitive information. Chambers USA has named Saikali a Nationwide Recognized Practitioner in Privacy and Data Security three years in a row, and he was named a Trailblazer in Cybersecurity by the National Law Journal. Saikali founded and is chair emeritus of the Sedona Conference's Working Group on Privacy and Data Security Liability. He holds the highest levels of data privacy certification with the International Association of Privacy Professionals

Robert Shimberg has provided compliance-related services and training for more than 300 businesses around the country. He assists clients from a variety of sectors in navigating responses to data breaches and cyber and ransomware attacks, including initial assessment, response options, liaison with law enforcement, asset recovery, required notice, interaction with third-party resources and litigation. Clients represented are in financial services, retail, restaurant groups, manufacturing, sales, automobile dealerships, law firms, trade associations and individuals.

Sarah Shullman is a recently appointed Palm Beach County judge. Previously, she was the South Florida Bureau Chief of the Florida Office of the Attorney General, where she conducted investigations and civil prosecutions of persons engaged in fraud and deceptive trade practices. Shullman also served Palm Beach County as a Civil Traffic Hearing Officer for the Fifteenth Judicial Circuit and practiced in business and finance litigation at Steel Hector & Davis and Squire, Sanders & Dempsey LLP.

Alice Vickers is a founding member of Florida Alliance for Consumer Protection and acts as director for FLACP. Vickers' career has been devoted to representing low-income citizens in housing and consumer issues through litigation and legislative advocacy. Before joining FLACP, she was a legal services attorney for 28 years. Most recently, Vickers has lobbied on behalf of Florida Consumer Action Network, PICO United Florida, and the Public Interest Law Section of The Florida Bar. The Consumer Protection Law Committee of The Florida Bar named Vickers the Consumer Protection Lawyer of the Year for 2013.

Chapter 1

Emerging Consumer Protection Issues in Light of Innovation and Technology Advancements

Supreme Court of Florida

500 South Duval Street
Tallahassee, Florida 32399-1925

MEMORANDUM

TO: Chief Judges of the District Courts of Appeal
Chief Judges of the Circuit Courts

FROM: Chief Justice Charles T. Canady Chas. T. Canady

DATE: May 11, 2020

SUBJECT: Best Practices

To assist judges in managing various challenges that may arise with proceedings during the pandemic, the Workgroup on Continuity of Court Operations and Proceedings During and After COVID-19 has developed best practices on the following topics:

- Facilitating Pro Se Litigants with Remote Appearance Technology, which sets forth best practices and logistical considerations regarding self-represented litigants who are appearing through remote technology;

- Representing Yourself and Using Remote Appearance Technology with the Courts, which contains helpful tips for self-represented litigants who are appearing through remote technology;

- Management of Evidence in Remote Hearings in Civil and Family Cases, which provides best practices and resources regarding the management of evidence during remote hearings in civil and family cases; and

- Out-of-County Inmates, which provides best practices on providing due process to out-of-county arrestees during the pandemic and includes sample forms.

Please distribute the attached best practices to all judges and the appropriate court staff in your respective jurisdiction and encourage them to make appropriate use of these helpful documents.

CTC:dgh

Attachments

cc: Justices
Judge Lisa Taylor Munyon, Workgroup Chair
DCA Clerks
DCA Marshals
Trial Court Administrators

COVID-19 WORKGROUP

CONTINUITY OF COURT OPERATIONS & PROCEEDINGS DURING AND AFTER

BEST PRACTICES

Facilitating Pro Se Litigants with Remote Appearance Technology

May 6, 2020

Introduction

This guide sets forth best practices and logistical considerations with respect to facilitating pro se litigants with remote appearance technology.

The court should be mindful of the following considerations:

1. Ensure the technology is sufficient to allow the court to preside over and resolve the matter effectively.
2. Leverage remote appearance solutions that present little or no cost to pro se litigants.
3. Recognize costs to the litigants of using phone minutes and/or data if free and stable Wi-Fi is not readily available to them.
4. Verify the required equipment needed for all participants, ease of use, and the ability to access the solution remotely.
5. Control access to the proceeding for participants and determine the necessary level of privacy required for the event.
6. Ideally, use the same mode of remote appearance technology for all parties participating in the court event.
7. Account for ADA requirements and web content accessibility standards.

Match each proceeding with the remote appearance medium that (1) complies with due process standards and general law, and (2) reliably achieves the purpose of the proceeding. In many instances a phone conference will satisfy the purpose of a court event, in others, a video conference may be required or preferable.

Best Practices for Judges

Planning for the Proceeding

1. Explore the full functionality of the remote appearance platform (i.e. waiting rooms) and attend regular training for the platform and other related technologies.
2. Allow for proper spacing and allotment of time for hearings, as pro se litigants may need extra time to present their case and work through any technology issues.
3. Ensure clear public information about the availability of non-confidential court proceedings via live streaming or other access.
4. When possible, obtain reliable email addresses for the parties, and verify their ability to access a stable internet connection if a video conference is to be used.
5. Determine whether any language interpretation will be needed by any participant, and the effect that need might have on effective participation via remote appearance technology. Schedule and group hearings to optimize the use of interpreter resources.

Noticing for the Proceeding

6. Provide notice to the litigant of the intent to use Zoom or similar free remote appearance platform along with connection instructions.
7. Require that notices of hearing contain a phone number and a link to the Zoom hearing, or similar free remote appearance platform, for the specified date and time.

Starting the Proceeding

8. Start each hearing by laying the ground rules. Describe how the hearing will be conducted and how the platform will be used.
9. Announce the case number prior to commencement of the proceeding and require all parties to announce themselves to assist with the court record, tagging, and transcription.
10. Address parties on the record to verify that they are waiving their right to be present in the courtroom for the proceedings. In addition, if there is a victim involved, ensure that the victim's rights are addressed on the record.
11. Assure all sides they will be heard, but that the use of the technology requires a rigid rule of speaking one-at-a-time. The judge will invite comment from each person and allow opportunities to respond. The judge runs the hearing and by name invites testimony, argument, etc. from each person so the record is clear and the hearing is orderly.
12. Despite not being physically in the courtroom, the court should continue to remind participants the proceeding is live, is being recorded, and that courtroom decorum rules apply.
13. The court should advise participants if the proceeding is being recorded and note restrictions on the unauthorized recording of the proceeding.

During the Proceeding

14. Judges should encourage the use of gallery view in the remote video settings, allowing all parties and participants to see each other in the hearing.
15. Be prepared to postpone the hearing if the pro se litigant has issues using the technology.
16. Finalize orders and file and serve through the CAPS Viewer or E-Portal.

Logistics

Contact Information / Procedures

1. Provide extra notice of hearings. Consider mailing the virtual hearing information to the pro se litigant with clear instructions on how to contact the court to arrange remote participation.
2. Provide a telephone option, toll-free if possible, as an alternative for video appearance if appropriate.

Procedural Practices

3. Judges and/or court staff must act as hosts to control remote meetings. Appoint the case manager or other staff as co-host so that they can help manage the waiting room and rename participants as needed.

Document Handling

4. Consider the need for an electronic signature workflow solution, with detailed instructions, when responding or filing.
5. Provide the capability for all parties to deliver all potential evidence to the court in advance.

Consider attaching the companion best practices guide, Representing Yourself and Using Remote Appearance Technology with the Courts, to pro se litigant communications. The companion guide has been posted to many court and clerk websites and shared with justice stakeholders.

Technology Features of the Remote Appearance Platform

6. When hosting hearings, the court should enable the "Waiting Room" function in Zoom. The "Waiting Room" allows the host to control who is admitted to the hearing and prevent participation by individuals who are not litigants in that case.
7. Train self-help staff and/or all staff so that they can troubleshoot with the pro se litigants. Provide a Zoom Procedure Guide to all staff.

COVID-19 WORKGROUP

CONTINUITY OF COURT OPERATIONS & PROCEEDINGS DURING AND AFTER

BEST PRACTICES

Representing Yourself and Using Remote Appearance Technology with the Courts

May 6, 2020

Remember, even though your hearing is happening over the phone or through the internet, it is a court proceeding. You should act the way you would if you were in the courtroom in person. Court rules and standards apply.

Please review the following tips:

Do:

- Do let the court know if you don't have a phone or access to the internet. The court may be able to help you find a way to participate or may postpone the hearing.
- Do visit the video call website (such as Zoom) or a video sharing website (YouTube) for guides, helpful videos, and additional information.
- Do prepare for your virtual hearing. If you plan to participate in your hearing by video, download the video application before your scheduled hearing. Be sure to test your speaker, microphone, and camera before the hearing. Video call software websites often provide a test link to try your equipment before the actual event (Zoom test example here).
- Do dress appropriately, like you would if actually going to the courthouse.
- Do limit distractions during your hearing. Put all pets and other things that may be a distraction in a different room. Find a quiet place to participate in the hearing.
- Do keep your device on mute when not speaking. Keeping your phone, mobile device, or computer on mute unless speaking reduces feedback and limits background noise.
- Do call the court in advance if you want to present evidence. If you have documents or witnesses you want available for your hearing, check the judge's website or call the court for more information.
- Do make sure others using your Wi-Fi network minimize their usage during your hearing so you have the best possible connection.

Don't:

- Don't ignore the virtual hearing. If you cannot make the hearing or have a conflict, notify the court.
- Don't talk over others, it makes it hard for the judge and others to hear. Wait to speak until asked to by the judge.
- Don't do other things while on the call. Just like in an actual courtroom, you must pay attention to make sure you don't miss something important that is said or something the judge asks you to do.

COVID-19 WORKGROUP

CONTINUITY OF COURT OPERATIONS & PROCEEDINGS DURING AND AFTER

BEST PRACTICES

Management of Evidence in Remote Hearings in Civil and Family Cases

May 5, 2020

Introduction

This guide sets forth best practices with respect to the management of evidence during remote hearings in civil and family cases, provides an overview of the requirements for the conduct of in-person and remote hearings specified in Florida Supreme Court Administrative Order 20-23, Amendment 1, and provides links to other resources generally addressing remote hearings.

Best Practices for Remote Evidentiary Hearings

Local administrative orders (AOs) should establish procedures for the filing and management of exhibits and the taking of witness testimony in remote hearings. Issues that a Florida judicial circuit may wish to address include specifying:

1. Procedures that distinguish between requirements for:
   a. Parties represented by counsel and self-represented parties, if appropriate; and
   b. Physical exhibits, exhibits capable of being provided electronically, and witness testimony.

2. Requirements for the parties to exchange exhibits and confer remotely before the hearing for the purpose of stipulating, as much as practicable, to the authenticity and admissibility of the exhibits. With respect to physical evidence, parties could be directed to exchange pictures of the evidence.

3. Requirements for the parties to file with the court any objections to exhibits by a specified deadline and procedures for the setting of hearings to resolve all such objections before the evidentiary hearing.

4. Requirements for the parties to:
   a. Exchange witness lists that include the witnesses' names, email addresses, and cell and landline phone numbers before the hearing;
   b. Ensure their witnesses who will lay the predicate for evidence have a copy of the evidence;
   c. Ensure their witnesses have the necessary technology to participate in the remote hearing and, if not, specify requirements for the provision of an affidavit from the party explaining and attesting to the inability for the witness to access such resources;

d. Ensure their witnesses are aware of the witness testimony protocol discussed below.
e. Meet specified deadlines for the provision of the witness lists to the court along with the identification of any witness for whom an interpreter or an accommodation under the Americans with Disabilities Act will be required or for whom they request sequestration. The name of the interpreter should be included in the witness list.

5. Requirements for the marking and indexing of exhibits, filing methods, e.g., via the clerk or ePortal, email to the presiding judge, or upload to a cloud storage service, and filing deadlines.
    a. With respect to physical evidence, the local AO could direct the parties to contact the presiding judge on a case-by-case basis and to indicate whether there is agreement among the parties as to how the physical evidence will be filed. Options for submission might include filing a picture of the physical evidence or submitting the evidence in a sealed, clear plastic bag.
    b. Consider advising parties that documents or other items that the presiding judge must review during the hearing, but which are not being submitted as evidence, e.g., a driver's license to verify identity, do not have to be provided to the judge in advance and may be presented to the judge during the hearing using the camera.

6. Any applicable limits on the time that will be allotted for the hearing.

7. Provisions indicating that:
    a. Discovery, evidence, and other rules of procedure still apply, unless suspended or amended by the Florida Supreme Court, as does the right to due process in all court proceedings; however, the courts and parties are encouraged to use flexibility during the public health emergency for the equitable resolution of cases.
    b. As such, nothing in the local AO limits the presiding judge's discretion to:
        i. Establish other procedures consistent with the AO;[1]
        ii. Admit or deny evidence in the case or determine other relief appropriate under the circumstances; and
        iii. Reset the hearing if technological issues prevent the meaningful review of evidence, where the parties have complied in good faith with the procedures, to use more appropriate electronic means or, if authorized

[1] In all cases, the presiding judge should ensure that any procedure independently established by the judge is equitable and does not result in an advantage to one party over the other.

under Florida Supreme Court AOSC 20-23, Amendment 1, for an in-person hearing.[2]

8. Provisions notifying parties that they should contact the presiding judge's office to determine whether the judge has established additional procedures for a remote hearing.

9. Provisions notifying parties of the suspension of certain rules, court orders, and opinions by Florida Supreme Court AOSC 20-23, Amendment 1, relating to remote hearings and remote administration of oaths.

10. Procedures that ensure the public's right of access to court hearings while maintaining any confidentiality that may apply to information in exhibits or witness testimony. [3]

11. Responsibilities of the parties for providing for the transcription of the record and indicating that court reporters may remotely participate in the hearing.

12. Post-hearing procedures for the filing of exhibits not filed before the hearing, for a corrected index of exhibits introduced in evidence, and for the parties to retain copies of evidence admitted or denied admission by the presiding judge until the resolution of the case and exhaustion of any appeal.

13. Sanctions applicable to a party's failure to comply with the requirements of the local AO. Consider including these sanctions in the presiding judge's standing order or order setting the hearing.

For examples of recent AOs on this topic, see Eleventh Judicial Circuit Administrative Memoranda.

Best Practices for Witnesses

With respect to witnesses, additional evidentiary issues for which the presiding judge of a remote hearing may wish to prepare include:

1. Advising witnesses at the beginning of the hearing or before their testimony of the following protocol for their testimony: they must be alone in a quiet room during their

[2] Under AOSC 20-23, Amendment 1, in-person hearings may be conducted only for essential proceedings. Additionally, under the AO, non-essential proceedings must be conducted remotely unless one of the two exceptions discussed in Footnote 4, below, apply.

[3] For a discussion of the strong presumption of openness for all court proceedings and of confidentiality requirements applicable in the judicial branch, see the Government-In-The-Sunshine-Manual, 2020 Edition, by the Office of the Attorney General, at pages 12-13 and 63-68, respectively. Although the public has a right of access, it does not have the right to participate in the proceeding.

testimony, may not use a virtual background, and are ordered, subject to contempt of court, to turn off all electronic devices except for the device enabling participation in the hearing and to refrain from exchanging any electronic messages during their testimony.

2. Requiring witnesses to remain in a Zoom waiting room until they are called to testify and removing them from the hearing following their testimony. To enable this function, the presiding judge or clerk must host the Zoom hearing. This functionality is critical in the event that a witness must remain in a waiting room because he or she is sequestered. If sequestration is necessary, one of the following options will be needed:
    a. The posting of a video of the proceeding after the hearing, rather than the live streaming the proceeding; or
    b. Determination of some other mechanism that ensures the witness is unable to view the live-streamed proceeding.
3. Confirming that the witness is alone by requiring him or her to use his or her camera to scan the room before and after testimony and noting this for the record.

Florida Supreme Court Administrative Order 20-23, Amendment 1

Florida Supreme Court Administrative Order 20-23, Amendment 1 requires the trial courts to conduct:

- Essential and critical proceedings in a manner that employs all methods feasible to minimize risk of COVID-19 exposure to all; and
- Non-essential and non-critical court proceedings using electronic means unless a judge determines that remote conduct of the proceeding is subject to an exception.[4]

Included within the categories of proceedings above are requirements for the conduct of certain proceedings in civil and family cases:

Civil and Family Essential Proceedings - *must be conducted remotely or in-person*	Civil and Family Non-Essential Proceedings – *must be conducted remotely*
Juvenile dependency shelter hearings	Alternative dispute resolution proceedings
Juvenile delinquency detention hearings	Status, case management, and pretrial conferences
Hearings on petitions for injunctions relating to safety of an individual	Non-evidentiary and evidentiary motion hearings
Hearings on petitions for risk protection orders	Hearings in juvenile delinquency cases

[4] The exceptions are that the remote conduct of the proceeding would be: (a) inconsistent with the United States or Florida Constitution, a statute, or a rule of court that has not been suspended by administrative order; or (b) infeasible because the court, the clerk, or other participant in a proceeding lacks the technological resources necessary to conduct the proceeding or, for reasons directly related to the state of emergency or the public health emergency, lacks the staff resources necessary to conduct the proceeding.

Hearings on petitions for the appointment of an emergency temporary guardian	Hearings in noncriminal traffic infraction cases
Hearings to determine whether an individual should be involuntarily committed under the Baker Act or the Marchman Act	Problem-solving court staffings, hearings, and wellness checks
Hearings on petitions for extraordinary writs as necessary to protect constitutional rights	Non-jury trials, except for juvenile delinquency and termination of parental rights petitions in dependency cases unless the parties in those cases agree to remote conduct

To facilitate the remote conduct of proceedings, the AO:

- Authorizes chief judges to establish temporary procedures for the use, to the maximum extent feasible, of communication equipment for the conduct of remote proceedings.
- Authorizes the remote administration of oaths by audio-video communication technology for witnesses.
- Suspends all rules of procedure, court orders, and opinions applicable to:
  - Court proceedings that limit or prohibit the use of communication equipment for conducting proceedings by remote electronic means; and
  - Remote testimony, depositions, and other legal testimony that limit or prohibit the use of audio-video communications equipment to administer oaths remotely or to witness the attestation of family law forms.

Other Resources Generally Addressing Remote Hearings

1. Florida:
   a. Video of a Remote Mock Trial, Seventeenth Judicial Circuit, posted May 1, 2020.
   b. Benchguide Checklist for Procedural Safeguards During Hearings for Judges, Eleventh Judicial Circuit, May 4, 2020: checklist addressing items that a judge should consider before and during a remote hearing conducted via Zoom.
   c. Zoom Script for Judge, Eleventh Judicial Circuit, May 4, 2020: script for judges that establishes ground rules for a Zoom hearing.

2. National Center for State Courts
   a. Checklist for judges in virtual proceedings, April 22, 2020: short checklist indicating issues to be considered by judges when conducting remote hearings.

3. Michigan's Virtual Court Resources: contains a variety of remote hearing resources, including:
   a. Trial Courts Virtual Courtroom Standards and Guidelines, April 17, 2020: guidance for the Michigan judiciary on the best practices for conducting remote hearings.

ORDER REQUIRING REMOTE/ELECTRONIC APPEARANCES

THIS CAUSE came before the Court on its own review pursuant to Supreme Court Order No. AOSC20-23 and local Administrative Order(s), and as part of reasonable temporary public health measures taken to assist with minimizing the spread of COVID-19; it is hereby

ORDERED through and until May 29, 2020, until otherwise amended or directed by Administrative Order, all parties shall appear for any scheduled hearing by video and/or phone conference.

For the **Small Claims Pre-Trial Conference and Mediation scheduled in this matter for May 7, 2020**, the parties **shall appear remotely through Zoom**, using the following steps:

1. **Each party may choose to appear by video or audio only**. Video is the preferred method as all parties will be placed with a mediator, at no cost, in order to attempt to settle your case on agreed terms. You do not need an account or to pay a fee to access Zoom. The Zoom App is available for free on IOS and Android devices, or via desktop computer. However, you may also appear through audio (phone or computer audio) only.
2. **For video appearance (preferred)**: after downloading the Zoom app, click on or type the Court's Zoom link here **https://zoom.us/j/7633959468 and enter Password 096642**. (Or, from your internet browser, go to https://zoom.us/join and enter Meeting ID 763-395-9468, Password 096642).
3. **For audio-only (phone)** appearances, dial (877) 853-5257 US Toll-free or (888) 475-4499 US Toll-free, and enter **Meeting ID 763-395-9468; Password 096642**.
4. **Please review the attached Important Information.**

As stated in your Summons, **failure to appear may result in default against you**. If any party does not have access to attend the Pre-Trial Conference or Mediation remotely, please contact the Court's Judicial Assistant at CAD-DivisionRE@pbcgov.org.

Pro Se litigants (appearing without an attorney) are encouraged to notify the Clerk of their email address and consent to receive documents electronically using the attached form. This information may also be emailed to CAD-DivisionRE@pbcgov.org. This will allow the Court to submit orders to the parties via email and communicate important information in a timely manner. Please see the Clerk's Website for instructions on how to register for and conduct e-filing: https://www.mypalmbeachclerk.com/court-services/e-filing/self-represented-filers.

All other information can be found on the Court's Divisional Instructions, updated frequently at https://www.15thcircuit.com/division/re/instructions.

DONE AND ORDERED in West Palm Beach, Palm Beach County, Florida. Tuesday, April 07, 2020

[% judge_signature %]

IMPORTANT INFORMATION REGARDING YOUR PRE-TRIAL CONFERENCE AND MEDIATION

The Fifteenth Judicial Circuit assures the public and legal community that the courts remain open, accessible, and operational to the fullest extent consistent with public safety. In accordance with the Florida Supreme Court's and 15th Judicial Circuit's Administrative Orders, Division RE is currently unable to hold hearings in person. To ensure access to the courts, Judge Shullman is proceeding with all scheduled events remotely through electronic means.

Accordingly, Division RE's **small claims pre-trial conferences and mediations are being held remotely**. **You may appear by video or audio (phone)**. However, failure to appear by either video or audio (phone) may result in sanctions, including dismissal or default.

The purpose of the pre-trial conference is to determine whether your case can be settled in mediation that day, or if it needs to be set for trial at a later date.

First step: Check-in.

At the beginning of your pre-trial conference, you will check-in with Judge Shullman and her Judicial Assistant by video or phone using the directions provided in the foregoing Order, and the process will be explained to you. Once you have been checked in, you don't have to control anything with your phone or computer except please wait patiently for your case to be called, as many are scheduled on the same day.

Second step: Virtual Mediation.

You will then be placed in a virtual breakout room to meet with a mediator at no cost to you. A mediator is a third-party neutral who has no interest in the outcome of your case; their only role is to help settle your case on terms agreeable to both parties, instead of taking your case to trial. Everything that happens at mediation is confidential. Your mediation will occur in a separate virtual room, which includes only the parties and mediator.

Third step: Sign mediation agreement and meet with Judge to approve. Or, set case for trial.

If an agreement is reached, you will be asked to sign your settlement agreement electronically. The mediator will help you do this. After mediation is complete, please stay in the meeting, you will be connected back to Judge Shullman electronically. Judge Shullman will then review, approve, and electronically sign your stipulation and order. At that point, your case is concluded and you will be free to leave the conference and comply with the terms of your agreement. A signed copy will be provided to you via mail or e-mail.

If an agreement is not reached, after mediation is complete, please stay in the meeting, you will be connected back to Judge Shullman electronically. At that time, Judge Shullman will set your case for trial and give you a date and time that you will return for that trial. A signed copy of the trial order with the date and time will be provided to you via mail or e-mail.

In either event, once you are connected with Judge Shullman you will have an opportunity to ask her any questions you have about your case (please note that Judges may not provide legal advice, however).

The Fifteenth Circuit understands this time is stressful for all parties. The Court is doing everything it can to ensure that you as a litigant have access to justice and an opportunity to be heard and have your day in court. If at any point you have any questions prior to your Pre-Trial Conference (other than requests for legal advice), please contact the Court's Judicial Assistant by email at CAD-DivisionRE@pbcgov.org. Please copy the other side on any communications to the Court.

ORDER REQUIRING REMOTE/ELECTRONIC APPEARANCES

THIS CAUSE came before the Court on its own review pursuant to Supreme Court Order No. AOSC20-23 and local Administrative Order(s), and as part of reasonable temporary public health measures taken to assist with minimizing the spread of COVID-19; it is hereby

ORDERED that until further notice, or as directed by Administrative Order, all parties shall appear for any scheduled hearing by phone and/or video conference. The parties may choose any provider so long as the parties agree and notify the Court sufficiently in advance of the hearing. Absent notification, the Court shall hold all hearings using Zoom.

The Court's Zoom link is https://zoom.us/j/7633959468 and Zoom Meeting ID is 763-395-9468; Password 096642. The Zoom App is available for free on IOS and Android devices, or via desktop computer. *You do not need an account or to pay a fee to use this service.* **All parties may choose to appear by phone, video or both. Video is preferred but not mandatory.** For phone-only appearances, dial (877) 853-5257 US Toll-free or (888) 475-4499 US Toll-free, and enter Meeting ID 763-395-9468; Password 096642.

If any party intends to introduce evidence or testimony, the parties must utilize video through Zoom or other videoconferencing platform, and must exchange evidence at least 48 hours in advance with a courtesy copy provided to the Court by email to CAD-DivisionRE@pbcgov.org.

All correspondence with the Court must be copied to all other parties. All motions, requests for relief and legal filings must be filed with the Clerk and a copy sent to all other parties.

All other information can be found on the Court's Divisional Instructions, updated frequently at https://www.15thcircuit.com/division/re/instructions.

Pro Se litigants (appearing without an attorney) are encouraged to notify the Clerk of their email address and consent to receive documents electronically using the attached form. This information may also be emailed to CAD-DivisionRE@pbcgov.org. This will allow the Court to submit orders to the parties via email and communicate in a timely manner. Please see the Clerk's Website for e-filing instructions: https://www.mypalmbeachclerk.com/court-services/e-filing/self-represented-filers.

DONE AND ORDERED in West Palm Beach, Palm Beach County, Florida. Wednesday, May 5, 2020

[% judge_signature %]

943.0415 Cybercrime Office.—There is created within the Department of Law Enforcement the Cybercrime Office. The office may:

(5) Consult with the Florida Digital Service ~~Division of State Technology~~ within the Department of Management Services in the adoption of rules relating to the information technology security provisions in s. 282.318.

Section 12. Effective January 1, 2021, section 559.952, Florida Statutes, is created to read:

559.952 Financial Technology Sandbox.—

(1) SHORT TITLE.—This section may be cited as the "Financial Technology Sandbox."

(2) CREATION OF THE FINANCIAL TECHNOLOGY SANDBOX.—There is created the Financial Technology Sandbox within the Office of Financial Regulation to allow financial technology innovators to test new products and services in a supervised, flexible regulatory sandbox using exceptions to specified general law and waivers of the corresponding rule requirements under defined conditions. The creation of a supervised, flexible regulatory sandbox provides a welcoming business environment for technology innovators and may lead to significant business growth.

(3) DEFINITIONS.—As used in this section, the term:

(a) "Business entity" means a domestic corporation or other organized domestic entity with a physical presence, other than that of a registered office or agent or virtual mailbox, in

this state.

(b) "Commission" means the Financial Services Commission.

(c) "Consumer" means a person in this state, whether a natural person or a business organization, who purchases, uses, receives, or enters into an agreement to purchase, use, or receive an innovative financial product or service made available through the Financial Technology Sandbox.

(d) "Control person" means an individual, a partnership, a corporation, a trust, or other organization that possesses the power, directly or indirectly, to direct the management or policies of a company, whether through ownership of securities, by contract, or through other means. A person is presumed to control a company if, with respect to a particular company, that person:

1. Is a director, a general partner, or an officer exercising executive responsibility or having similar status or functions;

2. Directly or indirectly may vote 10 percent or more of a class of a voting security or sell or direct the sale of 10 percent or more of a class of voting securities; or

3. In the case of a partnership, may receive upon dissolution or has contributed 10 percent or more of the capital.

(e) "Corresponding rule requirements" means the commission rules, or portions thereof, which implement the general laws

enumerated in paragraph (4)(a).

(f) "Financial product or service" means a product or service related to a consumer finance loan, as defined in s. 516.01, or a money transmitter or payment instrument seller, as those terms are defined in s. 560.103, including mediums of exchange that are in electronic or digital form, which is subject to the general laws enumerated in paragraph (4)(a) and corresponding rule requirements and which is under the jurisdiction of the office.

(g) "Financial Technology Sandbox" means the program created by this section which allows a licensee to make an innovative financial product or service available to consumers during a sandbox period through exceptions to general laws and waivers of corresponding rule requirements.

(h) "Innovative" means new or emerging technology, or new uses of existing technology, which provide a product, service, business model, or delivery mechanism to the public and which are not known to have a comparable offering in this state outside the Financial Technology Sandbox.

(i) "Licensee" means a business entity that has been approved by the office to participate in the Financial Technology Sandbox.

(j) "Office" means, unless the context clearly indicates otherwise, the Office of Financial Regulation.

(k) "Sandbox period" means the initial 24-month period in

which the office has authorized a licensee to make an innovative financial product or service available to consumers, and any extension granted pursuant to subsection (7).

(4) EXCEPTIONS TO GENERAL LAW AND WAIVERS OF RULE REQUIREMENTS.—

(a) Notwithstanding any other law, upon approval of a Financial Technology Sandbox application, the following provisions and corresponding rule requirements are not applicable to the licensee during the sandbox period:

1. Section 516.03(1), except for the application fee, the investigation fee, the requirement to provide the social security numbers of control persons, evidence of liquid assets of at least $25,000, and the office's authority to investigate the applicant's background. The office may prorate the license renewal fee for an extension granted under subsection (7).

2. Section 516.05(1) and (2), except that the office shall investigate the applicant's background.

3. Section 560.109, only to the extent that the section requires the office to examine a licensee at least once every 5 years.

4. Section 560.118(2).

5. Section 560.125(1), only to the extent that subsection would prohibit a licensee from engaging in the business of a money transmitter or payment instrument seller during the sandbox period.

6. Section 560.125(2), only to the extent that subsection would prohibit a licensee from appointing an authorized vendor during the sandbox period. Any authorized vendor of such a licensee during the sandbox period remains liable to the holder or remitter.

7. Section 560.128.

8. Section 560.141, except for s. 560.141(1)(a)1., 3., 7.-10. and (b), (c), and (d).

9. Section 560.142(1) and (2), except that the office may prorate, but may not entirely eliminate, the license renewal fees in s. 560.143 for an extension granted under subsection (7).

10. Section 560.143(2), only to the extent necessary for proration of the renewal fee under subparagraph 9.

11. Section 560.204(1), only to the extent that subsection would prohibit a licensee from engaging in, or advertising that it engages in, the selling or issuing of payment instruments or in the activity of a money transmitter during the sandbox period.

12. Section 560.205(2).

13. Section 560.208(2).

14. Section 560.209, only to the extent that the office may modify, but may not entirely eliminate, the net worth, corporate surety bond, and collateral deposit amounts required under that section. The modified amounts must be in such lower

amounts that the office determines to be commensurate with the factors under paragraph (5)(c) and the maximum number of consumers authorized to receive the financial product or service under this section.

(b) The office may approve a Financial Technology Sandbox application if one or more of the general laws enumerated in paragraph (a) currently prevent the innovative financial product or service from being made available to consumers and if all other requirements of this section are met.

(c) A licensee may conduct business through electronic means, including through the Internet or a software application.

(5) FINANCIAL TECHNOLOGY SANDBOX APPLICATION; STANDARDS FOR APPROVAL.—

(a) Before filing an application for licensure under this section, a substantially affected person may seek a declaratory statement pursuant to s. 120.565 regarding the applicability of a statute, a rule, or an agency order to the petitioner's particular set of circumstances or a variance or waiver of a rule pursuant to s. 120.542.

(b) Before making an innovative financial product or service available to consumers in the Financial Technology Sandbox, a business entity must file with the office an application for licensure under the Financial Technology Sandbox. The commission shall, by rule, prescribe the form and manner of the application and how the office will evaluate and

apply each of the factors specified in paragraph (c).

1. The application must specify each general law enumerated in paragraph (4)(a) which currently prevents the innovative financial product or service from being made available to consumers and the reasons why those provisions of general law prevent the innovative financial product or service from being made available to consumers.

2. The application must contain sufficient information for the office to evaluate the factors specified in paragraph (c).

3. An application submitted on behalf of a business entity must include evidence that the business entity has authorized the person to submit the application on behalf of the business entity intending to make an innovative financial product or service available to consumers.

4. The application must specify the maximum number of consumers, which may not exceed the number of consumers specified in paragraph (f), to whom the applicant proposes to provide the innovative financial product or service.

5. The application must include a proposed draft of the statement or statements meeting the requirements of paragraph (6)(b) which the applicant proposes to provide to consumers.

(c) The office shall approve or deny in writing a Financial Technology Sandbox application within 60 days after receiving the completed application. The office and the applicant may jointly agree to extend the time beyond 60 days.

Consistent with this section, the office may impose conditions on any approval. In deciding whether to approve or deny an application for licensure, the office must consider each of the following:

1. The nature of the innovative financial product or service proposed to be made available to consumers in the Financial Technology Sandbox, including all relevant technical details.

2. The potential risk to consumers and the methods that will be used to protect consumers and resolve complaints during the sandbox period.

3. The business plan proposed by the applicant, including company information, market analysis, and financial projections or pro forma financial statements, and evidence of the financial viability of the applicant.

4. Whether the applicant has the necessary personnel, adequate financial and technical expertise, and a sufficient plan to test, monitor, and assess the innovative financial product or service.

5. Whether any control person of the applicant, regardless of adjudication, has pled no contest to, has been convicted or found guilty of, or is currently under investigation for fraud, a state or federal securities violation, a property-based offense, or a crime involving moral turpitude or dishonest dealing, in which case the application to the Financial

Technology Sandbox must be denied.

6. A copy of the disclosures that will be provided to consumers under paragraph (6)(b).

7. The financial responsibility of the applicant and any control person, including whether the applicant or any control person has a history of unpaid liens, unpaid judgments, or other general history of nonpayment of legal debts, including, but not limited to, having been the subject of a petition for bankruptcy under the United States Bankruptcy Code within the past 7 calendar years.

8. Any other factor that the office determines to be relevant.

(d) The office may not approve an application if:

1. The applicant had a prior Financial Technology Sandbox application that was approved and that related to a substantially similar financial product or service;

2. Any control person of the applicant was substantially involved in the development, operation, or management with another Financial Technology Sandbox applicant whose application was approved and whose application related to a substantially similar financial product or service; or

3. The applicant or any control person has failed to affirmatively demonstrate financial responsibility.

(e) Upon approval of an application, the office shall notify the licensee that the licensee is exempt from the

provisions of general law enumerated in paragraph (4)(a) and the corresponding rule requirements during the sandbox period. The office shall post on its website notice of the approval of the application, a summary of the innovative financial product or service, and the contact information of the licensee.

(f) The office, on a case-by-case basis, shall specify the maximum number of consumers authorized to receive an innovative financial product or service, after consultation with the Financial Technology Sandbox applicant. The office may not authorize more than 15,000 consumers to receive the financial product or service until the licensee has filed the first report required under subsection (8). After the filing of that report, if the licensee demonstrates adequate financial capitalization, risk management processes, and management oversight, the office may authorize up to 25,000 consumers to receive the financial product or service.

(g) A licensee has a continuing obligation to promptly inform the office of any material change to the information provided under paragraph (b).

(6) OPERATION OF THE FINANCIAL TECHNOLOGY SANDBOX.—

(a) A licensee may make an innovative financial product or service available to consumers during the sandbox period.

(b)1. Before a consumer purchases, uses, receives, or enters into an agreement to purchase, use, or receive an innovative financial product or service through the Financial

Technology Sandbox, the licensee must provide a written statement of all of the following to the consumer:

a. The name and contact information of the licensee.

b. That the financial product or service has been authorized to be made available to consumers for a temporary period by the office, under the laws of this state.

c. That the state does not endorse the financial product or service.

d. That the financial product or service is undergoing testing, may not function as intended, and may entail financial risk.

e. That the licensee is not immune from civil liability for any losses or damages caused by the financial product or service.

f. The expected end date of the sandbox period.

g. The contact information for the office and notification that suspected legal violations, complaints, or other comments related to the financial product or service may be submitted to the office.

h. Any other statements or disclosures required by rule of the commission which are necessary to further the purposes of this section.

2. The written statement under subparagraph 1. must contain an acknowledgment from the consumer, which must be retained for the duration of the sandbox period by the licensee.

(c) The office may enter into an agreement with a state, federal, or foreign regulatory agency to allow licensees under the Financial Technology Sandbox to make their products or services available in other jurisdictions. The commission shall adopt rules to implement this paragraph.

(d) The office may examine the records of a licensee at any time, with or without prior notice.

(7) EXTENSION AND CONCLUSION OF SANDBOX PERIOD.—

(a) A licensee may apply for one extension of the initial 24-month sandbox period for 12 additional months for a purpose specified in subparagraph (b)1. or subparagraph (b)2. A complete application for an extension must be filed with the office at least 90 days before the conclusion of the initial sandbox period. The office shall approve or deny the application for extension in writing at least 35 days before the conclusion of the initial sandbox period. In determining whether to approve or deny an application for extension of the sandbox period, the office must, at a minimum, consider the current status of the factors previously considered under paragraph (5)(c).

(b) An application for an extension under paragraph (a) must cite one of the following reasons as the basis for the application and must provide all relevant supporting information:

1. Amendments to general law or rules are necessary to offer the innovative financial product or service in this state

permanently.

2. An application for a license that is required in order to offer the innovative financial product or service in this state permanently has been filed with the office and approval is pending.

(c) At least 30 days before the conclusion of the initial 24-month sandbox period or the extension, whichever is later, a licensee shall provide written notification to consumers regarding the conclusion of the initial sandbox period or the extension and may not make the financial product or service available to any new consumers after the conclusion of the initial sandbox period or the extension, whichever is later, until legal authority outside of the Financial Technology Sandbox exists for the licensee to make the financial product or service available to consumers. After the conclusion of the sandbox period or the extension, whichever is later, the business entity formerly licensed under the Financial Technology Sandbox may:

1. Collect and receive money owed to the business entity or pay money owed by the business entity, based on agreements with consumers made before the conclusion of the sandbox period or the extension.

2. Take necessary legal action.

3. Take other actions authorized by commission rule which are not inconsistent with this section.

(8) REPORT.—A licensee shall submit a report to the office twice a year as prescribed by commission rule. The report must, at a minimum, include financial reports and the number of consumers who have received the financial product or service.

(9) CONSTRUCTION.—A business entity whose Financial Technology Sandbox application is approved under this section:

(a) Is licensed under chapter 516, chapter 560, or both chapters 516 and 560, as applicable to the business entity's activities.

(b) Is subject to any provision of chapter 516 or chapter 560 not specifically excepted under paragraph (4)(a), as applicable to the business entity's activities, and must comply with such provisions.

(c) May not engage in activities authorized under part III of chapter 560, notwithstanding s. 560.204(2).

(10) VIOLATIONS AND PENALTIES.—

(a) A licensee who makes an innovative financial product or service available to consumers in the Financial Technology Sandbox remains subject to:

1. Civil damages for acts and omissions arising from or related to any innovative financial product or services provided or made available by the licensee or relating to this section.

2. All criminal and consumer protection laws and any other statute not specifically excepted under paragraph (4)(a).

(b)1. The office may, by order, revoke or suspend a

licensee's approval to participate in the Financial Technology Sandbox if:

a. The licensee has violated or refused to comply with this section, any statute not specifically excepted under paragraph (4)(a), a rule of the commission that has not been waived, an order of the office, or a condition placed by the office on the approval of the licensee's Financial Technology Sandbox application;

b. A fact or condition exists that, if it had existed or become known at the time that the Financial Technology Sandbox application was pending, would have warranted denial of the application or the imposition of material conditions;

c. A material error, false statement, misrepresentation, or material omission was made in the Financial Technology Sandbox application; or

d. After consultation with the licensee, the office determines that continued testing of the innovative financial product or service would:

(I) Be likely to harm consumers; or

(II) No longer serve the purposes of this section because of the financial or operational failure of the financial product or service.

2. Written notice of a revocation or suspension order made under subparagraph 1. must be served using any means authorized by law. If the notice relates to a suspension, the notice must

include any condition or remedial action that the licensee must complete before the office lifts the suspension.

(c) The office may refer any suspected violation of law to an appropriate state or federal agency for investigation, prosecution, civil penalties, and other appropriate enforcement action.

(d) If service of process on a licensee is not feasible, service on the office is deemed service on the licensee.

(11) RULES AND ORDERS.—

(a) The commission shall adopt rules to administer this section before approving any application under this section.

(b) The office may issue all necessary orders to enforce this section and may enforce these orders in accordance with chapter 120 or in any court of competent jurisdiction. These orders include, but are not limited to, orders for payment of restitution for harm suffered by consumers as a result of an innovative financial product or service.

Section 13. For the 2020-2021 fiscal year, the sum of $50,000 in nonrecurring funds is appropriated from the Administrative Trust Fund to the Office of Financial Regulation to implement s. 559.952, Florida Statutes, as created by this act.

Section 14. The creation of s. 559.952, Florida Statutes, and the appropriation to implement s. 559.952, Florida Statutes, by this act shall take effect only if CS/CS/HB 1393 or similar

legislation takes effect and if such legislation is adopted in the same legislative session or an extension thereof and becomes a law.

Section 15. Except as otherwise expressly provided in this act, this act shall take effect July 1, 2020.

Chapter 2

Data Privacy & Security Trends, Data Hostage Negotiations, & Cybercrime

Holland & Knight

Navigating Artificial Intelligence and Consumer Protection Laws in Wake of the COVID-19 Pandemic

April 16, 2020

Holland & Knight Alert

Kwamina Thomas Williford | Anthony E. DiResta | Esther D. Clovis

Highlights

- The Federal Trade Commission's (FTC) Bureau of Consumer Protection director issued a statement on Using Artificial Intelligence and Algorithms, providing added insight into how the FTC assesses a company's use of Artificial Intelligence and Algorithms (collectively AI).
- This statement comes in the midst of the COVID-19 pandemic during which there has been a wave of ingenuity unleashed, much of which implicate AI. COVID-19 tracking mechanisms, disinfecting robots, smart helmets, thermal camera-equipped drones and advanced facial recognition software are being considered and deployed in the fight against COVID-19.
- The FTC statement brings attention to the potential consumer protection exposure for companies – reaffirming that consumer protection laws in place for traditional human activity and automated decision-making technology will equally apply to sophisticated AI.

The Federal Trade Commission's (FTC) Bureau of Consumer Protection Director Andrew Smith issued a statement on Using Artificial Intelligence and Algorithms, providing added insight into how the FTC assesses a company's use of Artificial Intelligence and Algorithms (collectively AI). This statement comes in the midst of the COVID-19 pandemic during which we have seen a wave of ingenuity unleashed, much of which implicate AI. COVID-19 tracking mechanisms, disinfecting robots, smart helmets, thermal camera-equipped drones and advanced facial recognition software are being considered and deployed in the fight against COVID-19.[1]

These solutions may help save lives, but they also have consumer protection implications that must be considered. This FTC statement is timely and reminds us of the potential consumer protection exposure for companies – reaffirming that existing consumer protection laws covering traditional human activity and automated decision-making technology will equally apply to sophisticated AI. It further highlights how companies can manage the risk, emphasizing that the use of AI tools should be transparent, explainable, fair and empirically sound while fostering accountability.

Consumer Protection Risks Presented by AI

The FTC has long experience enforcing consumer protections presented by the use of data and algorithms that make decisions about consumers, and the statement reinforces the reality that such protections will be enforced in connection with AI technology. Front and center in the assessment will be traditional concepts of fairness, accuracy and transparency implicated by Section 5 of the FTC Act's prohibition against unfair and deceptive acts, equal protection laws such as the Equal Credit Opportunity Act (ECOA), and laws impacting consumer access to credit, employment and insurance such as the Fair Credit Reporting Act (FCRA).

Unfair and Deceptive Acts. Section 5(a) of the FTC Act protects against "unfair or deceptive acts or practices in or affecting commerce," and is often used to hold companies to fair and transparent privacy and security standards. For

example, in this time of crisis, people may be more willing to share personal information related to COVID-19 status and location for certain uses. This triggers numerous privacy concerns for consumers providing their sensitive information as well as responsibilities for companies collecting consumer data.

Nondiscrimination Laws. Equal opportunity laws, such as the ECOA and Title VII of the Civil Rights Act, protect consumers from being discriminated against on the basis of their race, gender, national origin or sex. With AI, we know that objective data (such as zip codes) may serve as a proxy for race, resulting in actionable disparate impact claims. In 2019, the federal government charged a social media and technology company with violating fair housing laws by enabling discrimination on its advertising platform under a disparate impact analysis.[2] Data is now surfacing that COVID-19 hospitalization rates and death rates appear to be disproportionally impacting black and Latino people.[3] If COVID-19 related data is used in connection with the extrapolation, prediction or access to healthcare, the utilization of such an algorithm could result in a disparate impact on these black and Latino communities if such disparities are not accounted for.

Fair Credit Reporting Act (FCRA). The FCRA protects information collected by consumer reporting agencies (CRAs) and sets strict notice, disclosure and investigation requirements around the use of such information. Companies should be aware if activities and use of AI could cause the company to be deemed a CRA or otherwise trigger obligations under the FCRA. For example, if the AI is being utilized to provide data about consumers or make decisions about consumer access to credit, employment, insurance, housing, government benefits or check-cashing, the company may be viewed as a CRA that must comply with the FCRA. This means taking diligent measures to ensure information is accurate, including providing consumers an opportunity to challenge inaccurate information. Similarly, if the company makes automated decisions based on data from a third party, an adverse action notice may be needed if the company's actions implicate the FCRA.

Managing Consumer Protection Risks Presented by AI

The FTC highlights several key principles that can help companies manage this risk. While the ultimate use of AI may not warrant strict adherence to these principles, they should be considered when managing risk.

1. **Be Transparent.** Don't deceive consumers about how you use automated tools. When collecting information from consumers, use clear messaging and conspicuous disclosures about what information is being collected, how it is going to be secured and stored, and how it is going to be used. If you change the terms of a deal or how information would impact a score based on automated tools, make sure to tell consumers.
2. **Explain Your Decision to the Consumer.** Understand that AI could trigger the FCRA, if it implicates the compilation of information and involves decisions being made related to consumer credit, employment or insurance. For example, if AI is used to assign risk scores to consumers, you should also disclose the key factors that affect the score, ranked in order of importance. If you deny consumers something of value based on algorithmic decision making, be prepared to explain why. Under this law, consumers must also have an opportunity to correct information used to make decisions about them.
3. **Ensure Decisions Are Fair.** Be sensitive to the disparate impact that your AI (or your products and services integrating AI)may have on protected classes. For example, given the disproportionate COVID-19-related hospitalizations and deaths that appear to be occurring in black and Latino communities, the use of COVID-19 related information in AI must be assessed and controlled for as a potential proxy for race. You should be mindful of such disparities on the front end, and tests should be done on the back end to assess whether there is a disparate impact on a protected class. If there is a disparate impact, you must ensure the impact is narrowly tailored to address the need.
4. **Ensure Data and Models Are Robust and Empirically Sound.** Make sure the AI models are validated and

revalidated to ensure they work as intended. Use acceptable statistical principals and methodology, and adjust as necessary to maintain predictability.

5. **Be Accountable.** The FTC suggests that the development of AI comes with a responsibility to be accountable for compliance, ethics, fairness and nondiscrimination. It suggests four key questions to ask for to help with such an assessment:
   a. How representative is your data set?
   b. Does your data model account for biases?
   c. How accurate are your predictions based on big data?
   d. Does your reliance on big data raise ethical or fairness concerns?

Perspective is key. Consider your accountability mechanism, and the prudence of using independent standards or expertise to step back and take stock of the new AI development. Finally, you should protect your algorithms from unauthorized use. This includes making clear what and how the algorithm should be used.

Conclusion: Takeaways

Innovation and AI will be needed to help our nation navigate these unprecedented times. While doing so, it is important that we keep in mind consumer protection laws. The FTC has made clear that traditional consumer protection laws will apply. Importantly, the statement does not specifically account for the differences between automated decision making and more sophisticated AI, the latter of which relies on machine learning and black box inputs that may be unknown. We will continue to follow developments in this area and whether the FTC's approach to such AI evolves over time. However, for now, companies should take heed of the current lens and expectations that the FTC will have when assessing AI. When it comes to consumer protection, understand the technology, understand its impact, understand your disclosure obligations and be accountable for what you put into the marketplace.

How Holland & Knight Can Help

Holland & Knight's Consumer Protection Defense and Compliance Team and Data Strategy, Security & Privacy Team work collaboratively to offer the full range of solutions our clients need to operate in today's data- and consumer-driven marketplace. Our seasoned professionals are committed to anticipate the risk management challenges our clients confront, develop appropriate compliance management systems, and advocate before the regulatory bodies and courts with the touch that is developed from having former roles in government agencies and credible reputations before decision-makers. For questions or more information about AI and consumer protection during this unprecedented COVID-19 pandemic, contact the authors.

Notes

[1] See BBC March 3, 2020, article, "Coronavirus: China's Tech Fights Back." See also NPR's April 10, 2020, article, "Apple and Google Build Smartphone Tool to Track COVID-19."

[2] See *HUD v. Facebook*.

[3] For example, in New York City, preliminary data from the Bureau of Communicable Disease Surveillance System shows that COVID-19 is killing black and Latino people at twice the rate it is killing white people.

Kwamina Thomas Williford is co-chair of the firm's Consumer Protection Defense and Compliance Team. Ms. Williford helps companies navigate complex regulations and enforcement regimes related to consumer engagement and interaction, including marketing and advertising, reporting and decisions being made based on consumer credit, receiving payments from consumers and the use of consumer information. She also advises companies on how to reduce their risk profile related to consumer protection concerns when looking to bring innovative products and technology to market.

202.828.1857 | kwamina.williford@hklaw.com

Anthony E. DiResta is a partner in Holland & Knight's Washington, D.C., office who is a nationally recognized leader with extensive experience in governmental consumer protection law enforcement investigations and litigation. A seasoned advocate, Mr. DiResta has assisted clients in bet-the-company governmental investigations and litigation pursued by federal agencies such as the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB) and the U.S. Department of Justice (DOJ), as well as in state enforcement proceedings involving state attorneys general.

202.469.5164 | Anthony.DiResta@hklaw.com

Esther D. Clovis is a New York attorney and a member of the firm's Litigation and Dispute Resolution Practice. Ms. Clovis has represented and counseled clients in user agreement disputes and consumer-based litigation in New York and New Jersey state courts, as well as New York federal courts. In addition, Ms. Clovis is an International Association of Privacy Professionals (IAPP) Certified Information Privacy Professional/United States (CIPP/US). She has counseled and assisted with the representation of corporate defendants in consumer class actions and complex litigation arising from alleged consumer privacy violations and allegations of data misuse. On the advisory side of her practice, Ms. Clovis supports the work of the Data Strategy, Security & Privacy team for clients revising their privacy policies and other online disclosures, as well as implementing the requirements of the California Consumer Privacy Act (CCPA) and other federal and state laws and regulations.

212.513.3549 | Esther.Clovis@hklaw.com

Holland & Knight

Cybersecurity, Common Sense, and COVID-19 (Coronavirus Disease 2019)

March 4, 2020

Holland & Knight Cybersecurity and Privacy Blog

Paul Bond

The Centers for Disease Control and Prevention (CDC) reports that it is "responding to an outbreak of respiratory disease caused by a novel (new) coronavirus that was first detected in China and which has now been detected in 60 locations internationally, including in the United States." While early steps are being taken to protect health and mitigate the spread of disease, cybercriminals have already taken advantage of public anxiety. A Washington State agency reports a phishing campaign in which the cybercriminals impersonate the CDC, "warning of new infections and promising to provide a list of active infections in the surrounding area if users click on a link." Clicking the link leads to the download of malware, with potential compromise of the device and associated workplace systems. The agency suggests that employers remind staff of anti-phishing protocol. These include exercising caution before opening emails from unknown parties, confirming the identity of senders via phone and not opening unexpected links or attachments.

Regardless of how COVID-19 progresses, companies should consider similar, common-sense measures to ready their cybersecurity preparedness for potential disruption. For example:

- if it is likely that employees will choose to work from home, reinforce applicable policies, procedures and training about home offices, protecting devices, encrypting data at rest, maintaining clear desk policies, etc.
- if executives will be out of the office, reinforce anti-spear phishing training with IT staff and others with access to sensitive company information
- use the occasion to update alternative contact information in data security breach response plans and other crisis communications plans
- for those same plans, develop redundancies if one or more key team members were to be out sick and unable to contribute – identify a flex squad
- consider making planned patches and upgrades now, before any potential disruption to workforce or supply chain
- look to complete any agreements needed for cybersecurity purposes on the same prompt schedule

By taking these steps to protect technology, companies may reduce the risk of loss that may otherwise accompany temporary disruptions like COVID-19 may prove to be.

DISCLAIMER: Please note that the situation surrounding COVID-19 is evolving and that the subject matter discussed in these publications may change on a daily basis. Please contact the author or your responsible Holland & Knight lawyer for timely advice.

Paul Bond is a litigation attorney who focuses his practice in the areas of data security, privacy and artificial intelligence. Mr. Bond helps clients make the best use of new technologies, including opportunities for automation, while identifying and managing the relevant risks.

215.252.9535 | Paul.Bond@hklaw.com

A Report on Businesses' Implementation of the California Consumer Privacy Act in the First Month

Holland & Knight

www.hklaw.com

California's landmark Consumer Privacy Act (CCPA) went into effect on January 1, 2020. A first-of-its-kind law in the United States, the CCPA grants California residents unique transparency into how covered businesses collect, use, and share consumers' online and offline personal information, and rights to access, delete, and object to the sale of their information.

Although the law passed in June 2018, businesses had to wait most of 2019 to see what the law would look like when it went into effect. Only in October 2019 did the Governor sign a series of amendments to add, *inter alia*, one-year partial exemptions for the personal information of employees and business-to-business situations. Just days later, the California Attorney General released draft regulations which significantly added to businesses' notice and recordkeeping obligations. On February 7, 2020, the Attorney General released a modified draft of the regulations. A final version of the regulations is still at least several weeks away.

Notwithstanding the lack of final guidance, the Attorney General begins enforcement of CCPA on July 1, 2020. In the meantime, businesses must balance the cost and resources of implementing the draft regulations, with the risk it could all be for naught if provisions are removed from the final requirements. Added to that uncertainty is a general lack of clarity around analytics and digital advertising technologies such as cookies and pixels, and particularly whether a company's ordinary use of those technologies on its website amounts to a "sale" of personal information under the CCPA.

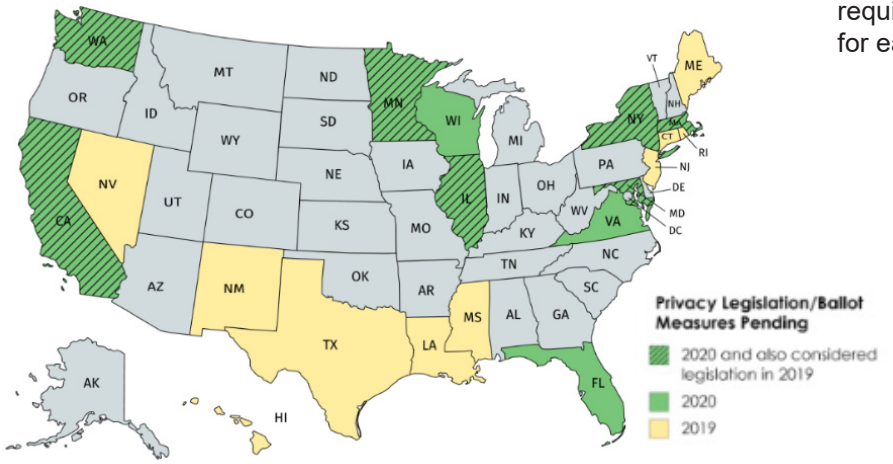
Two weeks after the law took effect, Holland & Knight conducted a survey of the websites of 125 of the country's largest public and privately-held companies to take stock of how businesses have operationalized CCPA.[1] The survey observed substantial differences in the approaches taken by companies, particularly in four key areas:

- Scope of Implementation
- Consumer Requests
- Do Not Sell
- Privacy Policy Updates

Scope of Implementation

Access and Deletion Rights Generally Exclusive to California

The passage of CCPA is directly traceable to the enactment of the General Data Protection Regulation (GDPR) by the European Union in May 2018. Similarly, CCPA inspired nearly twenty U.S. state legislatures to introduce equally comprehensive consumer privacy bills in 2019. So far this year, lawmakers in Florida, Illinois, Maryland, Massachusetts, Minnesota, New York, Virginia, Washington, and Wisconsin are all considering privacy legislation. Californians, of course, are likely to be considering Alastair Mactaggart's "CCPA 2.0" initiative on the State's November 2020 ballot.

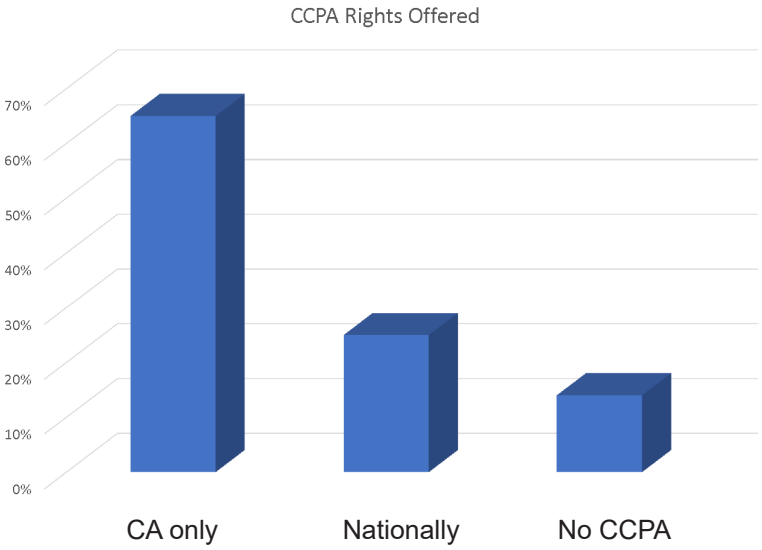


Despite widespread consumer interest in data privacy protections, and generally low expectations that the federal government could act to preempt state privacy laws in an election year, nearly 65% of companies surveyed limit the access, deletion and do not sell rights that form the core of CCPA to just California residents, rather than extend such rights voluntarily to additional jurisdictions that could adopt legislation but have not yet done so.

Just over 20% of companies give comprehensive access and deletion rights to consumers nationwide, regardless of residency. These include a diverse mix of retail, food and beverage, financial services, tech, and industrial businesses.

Nearly 15% of companies had made no website updates for CCPA at the time surveyed. These companies perhaps view the Act's July 1 enforcement date as the deadline for compliance. Any company that delays the rollout of CCPA's requirements, however, risks becoming a target for early and aggressive enforcement.

> "We will look kindly, given that we are an agency with limited resources, and we will look kindly on those [companies] that ... demonstrate an effort to comply … If they are not (operating properly) ... I will descend on them and make an example of them, to show that if you don't do it the right way, this is what is going to happen to you."
>
> - California Attorney General Xavier Becerra in an interview with Reuters on Dec. 10, 2019.



Consumer Requests

Submission Process

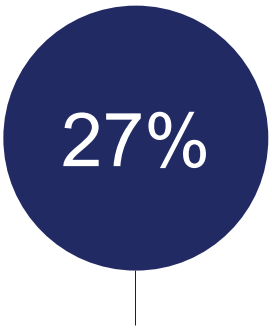
Even though only a small number of companies expressly grant access and deletion rights to consumers regardless of residency, in most cases, companies appear to lack a technical solution preventing non-California residents from submitting requests. Many rely on the consumer to self-confirm residency through a check box or statement of confirmation above the "Continue" button. Only one company was observed geo-fencing its CCPA request form to (presumably) California IP addresses.

The requirement in the October draft regulations that businesses provide a webform for submission of right to know requests was largely unexpected, and nearly a quarter of companies surveyed did not operationalize that requirement in January. Many instead provided consumers with only an email address for submission of requests. The choice appears to have paid off for some companies, as the modified regulations released in February eliminate the webform requirement and provide that email is an acceptable method for submission of requests. This change will particularly benefit companies with a global privacy program also covering GDPR, which only requires an email address for submission of consumer requests.

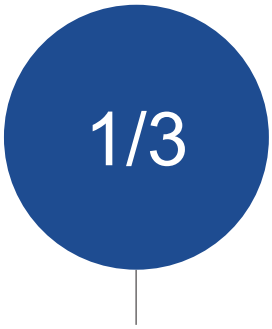
The requirement to provide a telephone option for consumers to submit requests received substantial feedback and commentary during the December 2019 public hearings held by the California Attorney General. This perhaps explains why 27% of companies do not currently offer a dedicated toll-free telephone number for submission of consumer requests. The February version of the regulations eliminates the telephone requirement for online-only businesses.

Authorized Agents Infrequently Mentioned

Only around 1/3 of companies mention in their privacy policy that consumer requests may be submitted by an authorized agent, or detail a special process by which an agent may submit a request on behalf of a data subject. As this was a new requirement in the draft regulations released in October 2019, we expect more companies will add such language in the round of updates made after the regulations are finalized.



of companies do not currently offer a dedicated toll-free telephone number for submission of consumer requests



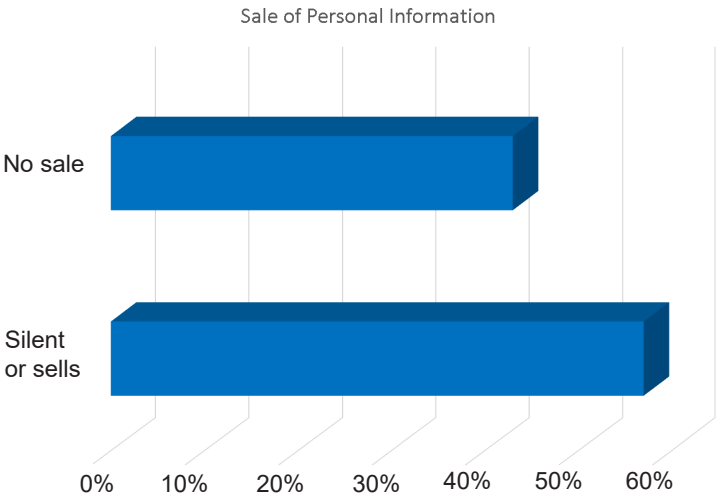
of companies mention in their privacy policy that requests may be submitted by an authorized agent

Do Not Sell

Approach Varies Widely — Blame Cookies

Navigating the ambiguity surrounding cookies and similar tracking technologies to operationalize CCPA's Do Not Sell requirement is one of the most challenging issues companies face and substantial differences were observed in implementation.

Only 22% of companies include a Do Not Sell link in their website footer at the time surveyed. In many cases, the link is connected to a GDPR-style self-serve cookie tool for consumers to manage cookie preferences on their own. In other cases, companies are effecting opt-out requests behind the scenes.



How and to what extent companies will utilize the Attorney General's newly-released CCPA button will be closely watched in the coming weeks.

While many companies (currently) do not have a CCPA opt-out link, less than 10% of companies actually state in their privacy policy that they "do not sell" personal information.[2] The remainder, 56%, are silent on the point, or more commonly, acknowledge they may sell personal information as defined under CCPA but do not provide consumers with a straightforward way to opt-out.

Cookies Policies Sporadically Used in the U.S.

Confusion around adtech is underscored by the fact that although no U.S. law requires a "cookie policy," 22% of companies provide consumers with a stand-alone cookie policy or policy on targeted advertising.

DNT = DNS

Further complicating matters, the modified regulations maintain the requirement that companies must treat user-enabled privacy controls as an opt-out of sharing. Under CalOPPA, businesses must state in their privacy policy whether they respect "do not track" signals or not. But because there is no industry standard for what amounts to "do not track," nearly all surveyed companies say they do not. The California Attorney General has now effectively eliminated that option, and companies will be forced to develop technical solutions to recognize and respond to "global" browser plugins, and privacy or device settings. Reg. § 999.315(d). How a company is expected to distinguish between California consumers' use of privacy controls versus other consumers' use, moreover, is a challenge that is likely to require significant industry resources to solve.

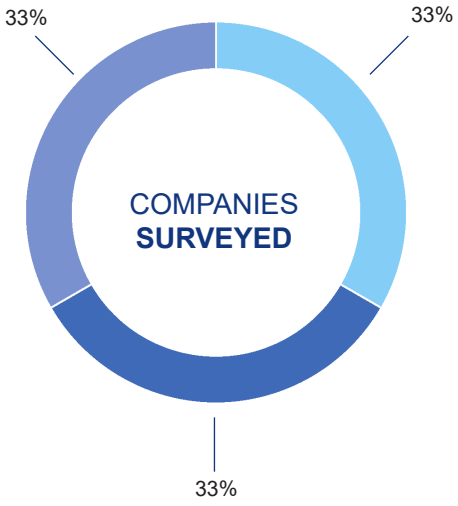
> The confusion around Do Not Sell is attributable to several factors: (1) a general lack of sophistication regarding third party behavioral advertising and website analytics on the part of the lawmakers, agency staff, and advocates who drafted the Act and regulations, and also by the lawyers and compliance personnel charged with implementing the law; (2) lack of real guidance from the California Attorney General on the opt-out process; (3) ambiguity in the law itself as to whether or when cookies-derived data constitutes a "sale" under the CCPA; and (4) technical and operational challenges that prevent a business from easily blocking third-party cookies on a user-by-user basis and communicating opt-outs to those third parties.

Privacy Policy Updates

Jurisdictional-Specific Disclosures

For companies with a global footprint, regional privacy regulations impose a unique compliance and operational challenge. Unsurprisingly then, the manner in which companies communicate jurisdiction-specific privacy disclosures to consumers varies widely.

One third of companies surveyed provide separate privacy policies applicable to consumers based on geographic region — generally the United States and Europe / Rest of the World. Another third take this jurisdiction-based approach a step further and provide a stand-alone California privacy notice, in addition to a U.S. privacy policy. At the other end of the spectrum, 1/3 of companies offer a global privacy policy intended to cover all applicable regulatory schemes in a single document.



provide separate privacy policies applicable to consumers based on geographic region

provide stand-alone California privacy notice, in addition to a U.S. privacy policy

offer a global privacy policy intended to cover all applicable regulatory schemes

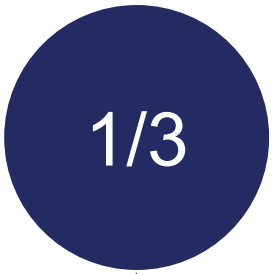
Nevada Disclosure

Fifteen percent of companies surveyed include language in their privacy policy in response to Nevada's new privacy law, NRS 603A.340. Interestingly, about half of those businesses say they do not sell under CCPA. The Nevada definition of a "sale" however, is encompassed within CCPA's broader definition of that term.

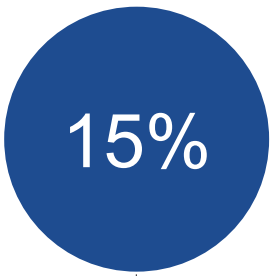
Notice of Financial Incentives

Just over half of the companies surveyed do not mention discrimination or financial incentives in their privacy policy. Of those that do, most address the new financial incentive language in section 999.307 of CCPA's draft regulations with a general statement that consumers will not be discriminated against for exercising their CCPA rights.

Fewer than ten companies acknowledge that they may charge a different rate or provide a different level of service. No surveyed company currently provides a "good faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference" and description of the method used to calculate such value, in its privacy policy. Reg. § 999.307(b)(5).



of companies mention in their privacy policy that requests may be submitted by an authorized agent



of companies surveyed provide Nevada opt-out

Conclusion

Most large companies committed significant time and resources towards CCPA compliance in 2019. But many businesses appear (reasonably) hesitant to expend additional resources implementing new requirements found in CCPA's draft regulations, or to make key decisions on the treatment of cookies, until the final form of the law is better understood.

The evolving regulatory landscape only complicates the challenges companies will face in the year to come. Federal action to preempt CCPA appears unlikely in the short term, and privacy advocates are pressing forward to have CCPA-author Alastair Mactaggart's "CCPA 2.0" initiative included on California's November 2020 ballot. At the same time, businesses are waiting to see what the State legislature will propose regarding the treatment of employees and other information exempted from CCPA for 2020. Outside of California, state lawmakers in some of the country's most populous states are considering comprehensive consumer privacy bills introduced during the first month of the year — several of which would be effective next year if enacted as currently drafted.

Practice Profile

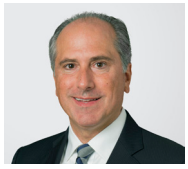
Holland & Knight's Data Strategy, Security & Privacy Team helps clients capitalize on data and tech capabilities while managing associated risks and incidents that arise. We have advised and represented clients on many of the largest public (and nonpublic) data issues and security incidents in the U.S.

We deliver: 1) pragmatic business-oriented solutions to address legal needs, 2) documentation you need for legal compliance and contracting, and 3) strategic representation during an incident, as well as in investigations and litigations that may follow. We do it efficiently, with transparent budgeting and billing.

How to Reach Us

Ashley L. Shively
Partner, San Francisco
415.743.6906
ashley.shively@hklaw.com

Mark H. Francis
Partner, New York
212.513.3572
mark.francis@hklaw.com



Mark S. Melodia
Partner, New York
212.513.3583
mark.melodia@hklaw.com

Paul Bond
Partner, Philadelphia
215.252.9535
paul.bond@hklaw.com

[1] It should be noted that this survey only reports on the publicly-available aspects of compliance and thus may not reflect the entire picture of a business's efforts to comply with the law.

[2] CCPA's draft regulations require a company that does not sell personal information state that fact in its privacy policy. Section 999.306(d)(2).

New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 261—NO. 45
FRIDAY, MARCH 8, 2019

Outside Counsel

Expert Analysis

Is 'Dittman' Creating a New Common Law Privacy Obligation on Employers?

BY FREDERICK D. BRAID, LOREN L. FORREST JR., MARK S. MELODIA AND NIPUN J. PATEL

The law has spent centuries chasing technological changes. Legal rules tend to evolve from the slow accumulation of precedent or from the difficult-to-find common ground of legislative consensus. And yet, the opportunities and risks created by society's technological hares race ahead without heed to the pace of the legal tortoises. Cybersecurity vulnerabilities at U.S. companies, and the resulting problems maintaining the privacy of personal information of employees, present the latest iteration of this age-old dilemma. Courts, legislatures and regulators have attempted to define the duties of employers concerning security and privacy, and this article explores the pros and cons of each approach. In the end, without regard to who is making the legal rules, the change is upon us and certain practical steps will best serve the interests of both employers and employees in this digital era.

The Common Law Approach

The recent Pennsylvania Supreme Court landmark decision in *Dittman v. UPMC*, established a common law duty on the part of Pennsylvania employers "to exercise reasonable care to safeguard its employees' sensitive personal information stored by the employer on an Internet-accessible computer system." 196 A.3d 1036, 1038 (Pa. 2018). The decision saved from dismissal a putative class action premised on claims of negligence and breach of implied contract. The employees claimed that their sensitive personal identifying information (PII) was stolen from UPMC following a criminal hack. Id. at 1038-39. The *Dittman* court held that Pennsylvania common law required employers who affirmatively undertake the collection and storage of their employees' sensitive PII to implement "reasonable care" and "adequate" security measures. Id. at 1048. The opinion suggests that the duty of reasonable care includes: encrypting, establishing "adequate" firewalls, and implementing "adequate authentication protocol[s]." Id.

The *Dittman* court expressly disavowed any intention to create new affirmative duties under the law; rather, it emphasized that the holding was applying the Restatement (Second) of

FREDERICK D. BRAID *is a partner at Holland & Knight, where he heads the labor, employment and benefits group.* LOREN L. FORREST JR. *is a partner in the group.* MARK S. MELODIA *is a privacy, data security and consumer class action defense partner, and* NIPUN J. PATEL *is a partner and trial lawyer at the firm.*

Torts §302 requiring protection and reasonable care where an actor engages in affirmative conduct. Id. However, as the *Dittman* court correctly observed in reviewing UPMC's arguments, the Pennsylvania Legislature, by statute, chose to create only a duty of notice on the part of employers experiencing breaches. See id. at 1041 (citing Pennsylvania's Data Breach Act, 73 P.S. §§2301-2309). Clearly then, *Dittman* does recognize obligations on the part of Pennsylvania employers not embodied by prior Pennsylvania statute or case law.

The Legislative/Regulatory Approach

While *Dittman* is a harbinger for judicially-created obligations, it can hardly be considered an outlier for employers given that New York (and other states) have enacted or proposed regulations or statutes that require covered employers to assess, maintain and/or develop cybersecurity programs. New York, like Pennsylvania, has a statute requiring virtually all employers to provide written notice of a data breach involving certain types of PII to both affected individuals and the NYS Attorney General's Office, the NYS Division of State Police; and the Department of State's Division of Consumer Protection. See N.Y. Gen. Bus. Law §899-aa. New York regulations go much further. The Superintendent of Financial Services promulgated 23 NYCRR Part 500, a "first-in-the-nation" regulation establishing comprehensive cybersecurity requirements for certain banks, insurance companies, and other financial services institutions regulated by the New York Department of Financial Services (DFS). 899-aa regulations require covered employers to maintain a comprehensive "cybersecurity program designed to protect consumers' private data; a written policy or policies that are approved by the board or a senior officer; a Chief Information Security Officer [CISO] to help protect data and systems; and controls and plans to help ensure [] safety and soundness … ." See id. The DFS regulations impose periodic compliance, audit, reporting, and self-certification deadlines by covered entities' CISO.

The New York State Attorney General's office has also proposed Stop Hacks and Improve Electronic Data Security (SHIELD) Act. The proposed SHIELD legislation requires covered entities to maintain "reasonable safeguards to protect the security, confidentiality, and integrity of" certain PII, including but not limited to disposal of data. The proposed SHIELD legislation includes various examples of required technical, personnel-based, and physical cybersecurity measures. Importantly, the SHIELD legislation attempted to provide safe harbors for compliance with: (a) federal or state regulations or (b) a third-party assessors' certification, provided there is no evidence of willful misconduct, bad faith, or gross negligence.

> Without regard to who is making the legal rules, the change is upon us and certain practical steps will best serve the interests of both employers and employees in this digital era.

Pre-dating these cyber-specific legislative/regulatory efforts, §203-d of the New York Labor Law restricts the use of employee PII by all NY employers. Section 203-d prohibits New York employers from publicly posting or displaying an employee's Social Security number; visibly printing a SSN on an identification badge or card, including any time card; placing SSNs in files with open access; and communicating an employee's PII to the general public.

Notably, PII is defined as information "including an employee's Social Security number, home address or telephone number, personal electronic mail (e-mail) address, Internet identification name or password, parent's surname prior to marriage, or driver's license number." Most employers in NY protect SSNs, but many forget the requirements for home addresses, phone numbers, and driver's license numbers.

Violations of §203-d require proof of a "knowing" violation of the statute, and resulting fines up to $500. "Knowing" is not an employer-friendly standard and will be inferred if the employer has not adopted policies or procedures to safeguard against §203-d violations. Violations may be assessed where an employer lacks procedures to notify certain employees of these provisions. Proper training and education of employees is, therefore, a key safeguard against violations of §203-d. Indeed, many employers do not have procedures in place to limit access to employee PII to only those employees whose jobs actually require such access, typically a small percentage of the workforce.

Contrasting §203-d with the *Dittman* case, 899-aa and the proposed SHIELD legislation, it is clear that §203-d's provisions are limited to employee PII, whereas 899-aa and SHIELD encompass more robust protections for a greater range of PII, not just employee PII. Further, the limited scope of §203-d and the minimal penalties of $500 explain why 899-aa was enacted and SHIELD was proposed by NY's legislature with more comprehensive remedies.

The Preferred Approach

Dittman's common law approach of dealing with cybersecurity programs and data breaches leaves much to be desired. First, *Dittman* provides no guidance on what may be considered "adequate" or

"reasonable" cybersecurity measures for employee PII. Second, *Dittman* holds that the question of adequacy is essentially one of fact, inappropriate for resolution at the dispositive motion stage, likely answerable only after costly discovery (including, presumably, the cost of expert witness reports). Third, adequate compliance is left to second-guessing by plaintiffs' lawyers and trial judges who not only will likely lack the technical expertise to make such assessments, but may be asked to do so several months or even years after a breach takes place. Lastly, unlike the DFS regulations, *Dittman*'s broad strokes do not provide for safe harbors or exemptions for smaller employers.

New York's regulations are far from perfect. However, they do attempt to provide explicit guidelines for compliance, and a set of best practices and principles from which employers can proactively attempt to craft measures to protect employees' PII and mitigate the risk of breach events. Moreover, those regulations encourage periodic reassessment and independent audit of cybersecurity programs, together with mechanisms for employers to obtain periodic feedback from the regulators themselves. Other states' statutes, including Ohio, provide an affirmative defense against tort liability to companies who adequately comply with detailed cybersecurity regulations similar to those embodied in the DFS regulations and proposed SHIELD law. Thus, proactive legislative guidance would serve employees, employers, and the public much better than protracted ad hoc common law development of legal requirements.

What's an Employer to Do?

Cyberattacks and data breaches implicating employee PII are unlikely to go away anytime soon. Thus, regardless of jurisdiction or size, employers must recognize that the evolving legal landscape calls for action and self-evaluation. *Dittman* only underscores that cybersecurity obligations on employers are the new norm.

• **Assess the potential threat.** Start proactive compliance measures by assessing the process for collection and retention of current, prospective, and former employee PII. How much employee PII is the company taking in? Is it all necessary? How and where is the PII being stored after collection? For what length of time? Is that length of time consistent with the company's written retention schedules? Is that timing appropriate/necessary?

Cyberattacks and data breaches implicating employee PII are unlikely to go away anytime soon. Thus, regardless of jurisdiction or size, employers must recognize that the evolving legal landscape calls for action and self-evaluation. 'Dittman' only underscores that cybersecurity obligations on employers are the new norm.

• **Assess the safeguards.** In addition to assessing risk, employers should assess safety. Has the company adopted written security procedures to ensure protection of any stored PII? How comprehensive are the procedures? Are employees trained on the procedures? Have relevant stakeholders from legal, IT, and HR all been given an opportunity to weigh in on and propose changes to current security measures? Is someone responsible for periodic reassessment and review?

• **Conduct an audit of the safeguards.** Safeguards are only as good as the employees who follow them. Thus, it is important for employers to ask whether employees who have been trained on security procedures are following them? Do they understand the training they received? How often are employees being retrained and/or is the training itself being refreshed? How strong or vulnerable are technical procedural safeguards like encryption, firewalls, and authentication protocols? How often are independent audits of those safeguards being conducted?

• **Develop a plan.** Regardless of however strong the company's safeguards may be, it should be ready to confront a breach if it occurs. Does the company have an organized, step by step process to assess the scope of a potential breach? Is a written plan in place to ensure compliance with any state notification laws in the event of a breach? Has the company developed written risk-mitigation steps to implement post-breach in order to minimize the financial, legal, PR, employee relations, and other risks it may face post-breach?

• **Insurance.** Insurance can be a powerful financial risk mitigation tool to minimize the disruption and business impact of a data breach. Has the company purchased cyber insurance? Are the cyber policies broad enough to cover breaches of employee PII? Potential lawsuits arising out of same? Judgments? Legal fees?

Data Strategy, Security & Privacy Team

ANNOUNCEMENT

May 2020

To our colleagues, clients and friends,

The world today has no shortage of complex problems. As the head of Holland & Knight's **Data Strategy, Security & Privacy Team**, I am pleased to offer a four-part series of teleseminars designed to simplify and solve challenges at the intersection of law and technology. Each of these 1.5-hour sessions provides practical guidance for the business owner, digital product developer, marketer or the compliance, risk and legal professionals who advise them. The real-life scenarios featured include handling a data breach and ransomware demand, strategies and tactics for complex tech negotiations, managing risks when launching a website and mobile app, as well as spotting and mitigating risks in the use, deployment or development of artificial intelligence. At a moment when we are maximally dependent on video conferencing, social media and e-commerce platforms, our team hopes that this helps your team.

Originally developed as an internal CLE resource, and launched and conducted during stay-at-home orders, these programs show how Holland & Knight attorneys can help businesses get things done even in the most difficult of circumstances. As always, please reach out to any of our experienced legal professionals with any questions regarding cybersecurity or data compliance matters. We look forward to reconnecting with you *offline* in the near future.

Best,

Mark S. Melodia
Leader, Data Strategy, Security & Privacy Team

2020 Data Boot Camp Series

Below are the descriptions and registration links for each session in the four-part series. You will need to separately register for each session and complete it to receive CLE credit for that session. If you have any issues when registering, please email our **Webinars Team** for assistance.

Navigating a Data Breach Response

Presenters: **Paul Bond**, **Adam Bookbinder**, **Shannon Hartsfield** and **Thomas Bentz**
90 Minutes

Topics:

- Incident response planning and mock incident training
- Counsel's role
- Maintaining attorney-client privilege and working with cyber insurance carriers
- Advising on legal obligations: security requirements and data breach notification laws, as well as special considerations for financial institutions, Health Insurance Portability and Accountability Act (HIPAA)-covered entities, merchants accepting payment cards and companies doing business in the European Union
- Managing legal and business exposure, and preparing for privacy litigation

Register to view this webinar. Download the **presentation materials** prior to starting the webinar.

Contracting Data Rights, Data Privacy and Cybersecurity

Presenters: **Maximillian Bodoin**, **Robert Hill** and **Mark Francis**
90 Minutes

Topics:

- Understanding the supply chain and third-party risk management
- Market standards for data rights, data privacy and cybersecurity
- Understanding customer vs. service provider perspectives
- Checklists, negotiation strategies and fallback positions
- Liability and indemnity: resolving risk allocation disputes

Register to view this webinar.

Managing Legal Risks in Online Business Activities

Presenters: **Ashley Shively**, **Paul Bond** and **Joel Roberson**
90 minutes

Topics:

- Understanding and drafting online privacy policies and terms of use
- Understanding the context: websites, mobile apps and other online services
- Special concerns in monetizing consumer data and risks around minors
- Privacy laws: Federal Trade Commission Section 5, CAN-SPAM Act, Telephone Consumer Protection Act, Children's Online Privacy Protection Act, California Online Privacy Protection Act, California Consumer Privacy Act and the EU's General Data Protection Regulation

Register to view this webinar.

Engaging with Clients on Artificial Intelligence Issues

Presenters: Ieuan Mahony, Kwamina Williford and Mark Francis
90 minutes

Topics:

- How AI works
- Ownership and use of the AI engine
- Ownership and use of AI data
- AI in the law: managing legal bias and other risks

Register to view this webinar.

Continuing Legal Education (CLE)

Holland & Knight is an approved CLE provider in several jurisdictions, including California, Georgia, Illinois, and New York. All reasonable efforts to seek CLE credits for this program will be made. In certain instances, some programs may not be awarded CLE credits because of either content or jurisdictional restrictions. For New York attorneys, this program's format qualifies for CLE for transitional (newly admitted) and experienced attorneys.

About the Data Strategy, Security & Privacy Team

Holland & Knight's Data Strategy, Security & Privacy Team offers the full range of solutions companies need to operate in today's data-driven marketplace. The team has the broad set of litigation, legislative, legal, compliance, crisis management and technical experience required to develop holistic, tailored solutions for clients. The firm offers true one-shop capabilities with its full-service practice that addresses even the most complex cybersecurity and privacy issues.

Connect With Us:

Holland & Knight
www.hklaw.com

Holland & Knight LLP | Operations Center | 524 Grand Regency Blvd. | Brandon, FL 33510-3931 | www.hklaw.com

February 1, 2018

White Paper

Blockchain and Distributed Ledger Technology: *An Analysis of its Impact on the Syndicated Loan Market*

Part One: General Considerations and Blockchain Primer

Table of Contents

EXECUTIVE SUMMARY[1]

Loan Syndications and Trading Association (the "**LSTA**") is the trade association in the United States for loan market participants active in the syndicated loan market. The LSTA has produced a white paper to assist its membership in anticipating how blockchain and distributed ledger technology ("**DLT**") will impact the industry. In addition to practical considerations, this paper includes an analysis of the legal and policy considerations that members of the industry should consider as they approach DLT technology.

This White Paper is broken up into three parts. The first part provides a brief description of the loan market and a primer on blockchain and DLT, including several protocols under active development that have potential application in the loan market. We also provide a comparison of these protocols to the most popular public blockchain networks—Bitcoin and Ethereum. The second part provides a detailed breakdown of "smart contracts"—the term commonly used to describe computer code that makes up decentralized applications—which have the most relevance to the loan market. This will include a discussion about the evolving thoughts of technologists and computer scientists around the relationship between human prose and computer code. Much of this discussion has particular relevance to the financial industry because of the industry's heavy reliance on extensible mark-up languages ("**XML**"), such as FpML. In contrast, the DLT industry's focus continues to be on general purpose programming languages, like Kotlin, Go and Solidity. The third part addresses the specific use cases likely to benefit from DLT and smart contracts, including loan origination in the primary loan market, secondary loan market and OFAC and KYC verification.

This paper and the research behind it should serve as a useful tool for educating members about blockchain and DLT. It is also our hope that it will lay the foundation for the LSTA, working closely with its members, to develop a general framework for implementing solutions that can address the entire lifecycle of syndicated loans, from origination to repayment. With this framework in place, the industry can begin to tackle existing (and anticipated) legal and regulatory requirements that will affect the deployment of DLT in the industry. These include regulations applicable to data security and privacy laws, KYC and anti-money laundering requirements and the general enforceability of smart contracts, both in the US and abroad. Although this paper was produced within the context of the US legal and regulatory environment, much of the information and work product contained herein are equally important in other loan markets, including in the UK and Europe.

[1] This report was prepared for the LSTA by Holland & Knight LLP.

EXISTING PRACTICES

ROLE OF THE LSTA

There is no single regulatory authority charged with the responsibility of regulating the syndicated loan market in the US. Of course, most participants within the loan market are regulated institutions that have one or more regulators overseeing their activities, but the loan market itself is not regulated. The LSTA is, therefore, the entity to which loan market participants turn for standard forms, best practices, and general assistance with loan transactions.

The LSTA maintains a library of documents that can be used by market participants in the origination, servicing and trading of loans in the Loan Market. The forms which the LSTA has promulgated for use in the primary market such as the LSTA's Model Credit Agreement Provisions have been widely adopted by market participants. The LSTA's secondary trading documents, including the LSTA's Par / Near Trade Confirmation (the "**Confirm**"), are the standard forms used by loan market participants for trading and settling loan trades.

TRADITIONAL TRADE MECHANICS

The LSTA's suite of secondary trading documents, including the Confirm which is used to trade performing loans, are used by all loan market participants to evidence their loan trades and then settle those trades (under New York law, loan trades need not be in writing to be enforceable; however LSTA best practices provide that those trades should be evidenced on a Confirm). A loan trade will typically settle as an assignment where the buyer then becomes a lender of record under the credit agreement. Depending on certain circumstances, a loan trade may not be capable of settling as an assignment, and instead, the parties must seek to settle their trade as a participation. Provided parties settle their trade on the LSTA's Form of Participation Agreement, that participation will generally be afforded sale accounting treatment. Accordingly, the rule defaulting to a participation arrangement is not seen as creating any material credit risk or otherwise affecting the economics of the trade.

INTERESTED PARTIES IN A TRANSACTION

In the primary loan market, there are several interested parties involved in the origination of any large syndicated loan. There will be (i) one or more borrowers to whom the loan is made and where primary responsibility for loan repayment lies under the terms of the credit agreement, (ii) one or more lenders in the syndicate each of whom owns a portion of the loan, and (iii) an administrative agent who is responsible for the ongoing administration of the loan. In addition to these parties, there may also be other parties involved in the making of a loan, including a lead arranger who leads the structuring and syndication of the loan, parties adding credit enhancement (e.g., a party acting as a guarantor of the loan), holders of subordinated tranches of debt, and providers of interest rate hedges. There are also relevant service providers in the loan market, including ratings agencies and the CUSIP Service Bureau.

In the secondary loan market, each loan trade has a selling lender and a legal entity seeking to buy the loan, an administrative agent who must acknowledge or consent to the loan assignment, and, of course, a borrower whose consent to the loan trade is also typically required. The buyer and seller execute a Confirm to evidence their loan trade and the relevant form of assignment agreement pursuant to which the loan is assigned to the buyer.

To properly design a DLT solution, each party must be accounted for with respect to (i) its participation in any formal governance documents required to participate in a DLT, (ii) creating data structures that model the attributes of that party necessary to engage in digital transactions (e.g., name, taxpayer identification number, state of organization, and role in transaction), and (iii) determining what level of permission each participant within the DLT has with respect to each item of information maintained on the ledger. We will discuss each of these three contexts in more detail below, but as a preliminary observation, context (ii) is similar to the exercise that is necessary when designing any database. On the other hand, context (i) and the nature of context (iii) require an approach that is unique to distributed ledgers, as will become more apparent later in this report.

BLOCKCHAIN AND DLT MECHANICS

THE BASICS

Block or No Block

As a preliminary consideration, it is useful to address the confusion around the terms "distributed ledger" and "blockchain." Generally, these two terms are used interchangeably by most people—even by some within the industry. From a technical perspective, blockchains are one type of distributed ledger, which are distinguishable by their use of a data structure referred to as a "block". These blocks contain a number of transactions, which when processed into a block, are then cryptographically hashed—meaning a cryptographic algorithm is applied to the block, which returns a deterministic value. The resulting value of that hash is then included as a part of the next block, so that all of the blocks on the blockchain are cryptographically linked. The effect of this is to make it increasingly difficult to change any aspect of a block as more blocks are added—as a change to one block has a cascading effect on every subsequent block. This has led some to argue that blockchains are more secure than non-blockchain DLT networks. Although that may be the case for certain protocols and network configurations, there are many circumstances where a blockchain affords no appreciable increase in the security or integrity of the network. Because this distinction has little relevance to the application of DLT to the loan market, we will use the terms interchangeably.

Maintaining a Ledger

What both blockchains and DLT do share is a decentralized peer-to-peer network that maintains a ledger of transactions that utilizes cryptographic tools to maintain the integrity of transactions and some method of protocol-wide consensus to maintain the integrity of the ledger itself. Although many networks have sophisticated and robust ledgers, it is easiest to think of a ledger as a simple database or Excel spreadsheet that can store information (e.g., someone's name, age, address, and date of birth). Perhaps most importantly, these ledgers are replicated across potentially thousands of computers—known as nodes—all connected to a common network over the internet. With some exceptions that will be discussed later, the replicated ledger on each node will maintain a complete and identical history of every transaction validated on that network.

Decentralized Architecture

The concept of a decentralized architecture, as used in DLT, is often a point of confusion. The concept arises out of the way several aspects of DLT result in a network having no single point of failure. This is not possible with a centralized server-based approach but is possible when the data on the server is replicated on every node. The

network protocol requires all nodes to operate under the same set of rules (a "protocol"), which are embodied in computer code running on every node. Without this common protocol, there would be no way to ensure that every node's ledger is being updated in a manner consistent with all the other nodes. Put in slightly different terms, it is a network of computers, all running the same software, that must come to agreement upon whether a change to the network's ledger should be made, and if so, what that change should be. Although it may sound complicated, this process is almost completely invisible to the user.

Transacting across a Peer-to-Peer Network

Updating the ledger on a network is an event usually initiated by one node (e.g., send one unit of virtual currency to the following address)—often referred to as a "transaction". The initiating node is generally not connected to every node on the network. In fact, a node on the Bitcoin network may only be connected to twenty or twenty-five nodes out of several thousand. As the initial set of peer nodes receive the transaction from the initiating node, each node confirms the transaction is in proper form. If validated, each of these nodes, which are connected to their own set of peers, re-broadcasts the transaction to its peers. This process repeats itself until eventually every node on the network has received the transaction. After the transaction has propagated throughout the network, there is still one last step in order to complete the transaction—the transaction must be recorded on the ledger. In the case of a blockchain network, that means the transaction will be aggregated with other transactions and included in a new block.

The transactions included in a block do not necessarily have any relationship to each other, other than a temporal one. For those DLT networks that do not implement a blockchain, transactions still need to be logged on the network's ledger through some mechanism to reach consensus. We will discuss these alternative ledgers and consensus mechanisms below.

PUBLIC VS. PERMISSIONED LEDGERS

Before proceeding any further, it is important to note that DLT can be implemented with or without access controls. There are open, public networks and restricted, permissioned networks. As its name suggests, an open, public network is open to the public, who can query the ledger and broadcast transactions without any authorization. In contrast, a closed, permissioned network is restricted to specific individuals who have received credentials from a trusted third party. The effect of these two types of networks is that transactions recorded on a public blockchain are generally open for public query, while transactions on a permissioned blockchain can only be seen and executed by those individuals explicitly granted permission to do so. Of course, even on a public network, transactions can be obfuscated by cryptography and other techniques (e.g., zero knowledge proofs) so that only certain individuals can see certain transactions recorded on a public ledger.

Naturally, financial institutions have concerns about using publicly accessible databases to conduct transactions involving customer information. This concern has led many financial institutions to focus on permissioned blockchains. Another potential issue with a public ledger is the fact that anyone can operate a node or run a miner on a public blockchain network. Arguably, these individuals should be subject to a financial institution's Know Your Customer (KYC) and Bank Secrecy Act (BSA) requirements—something that is not possible (or desirable) with respect to public networks. Nevertheless, some public blockchain advocates argue that permissioned systems cannot provide the reliability that an open network provides. Proponents of this position argue that permissioned ledgers lack the robust network that ensures that no single point of failure can disrupt the network. There is merit

to this argument, as there can be an inverse relationship between the number of nodes operating on a given protocol and the risk of a security breach, which is discussed in more detail below. For example, the authority responsible for issuing credentials on a permissioned system is seen by many as a central point of failure.

Although this debate will likely go on for years, it seems unlikely that financial institutions will integrate their systems with public networks, at least not initially. As such, we will spend the rest of this first part of our White Paper highlighting the different consensus mechanisms and protocols—specifically focusing on the differences between the permissioned systems likely to be initially adopted by the industry versus their public counterparts. In the long-run, it is possible that permissioned systems will eventually evolve into public networks, resulting in a massive, globally interconnected blockchain network.

CONSENSUS MECHANISMS: PROOF OF WORK, PROOF OF STAKE AND BFT

Certain nodes on a network are responsible for validating transactions and helping to maintain consensus—the term given to the concept of all nodes on a network reaching agreement on updates to the network's ledger. These nodes, however, must be capable of working in a trustless manner. Accordingly, a solution is necessary for what is often called the "Byzantine generals' problem." This refers to the dilemma faced by Byzantine-era generals on how to coordinate during battle when the lines of communication may be compromised, such that the information they receive is meant to deceive them. The solution requires that trust be removed from the process. There are several approaches to solving this problem in the context of blockchain. The most reliable, at least on public blockchains, is a technique called "proof-of-work" or "PoW". PoW involves a process called "mining" performed by special nodes called "miners". It is an approach that has kept the Bitcoin network secure for the past nine years (not to be confused with Mt. Gox and others who have suffered losses because their internal systems were hacked).

Proof-of-Work

In addition to propagating transactions, miners are responsible for creating new blocks that are added to the blockchain. In order to promote a robust network of mining nodes, blockchain protocols provide incentives to miners by issuing them newly issued cryptocurrency (e.g., bitcoin) if they are the first to successfully mine a block. Mining requires the miner to apply intensive computational efforts towards solving a random mathematical puzzle. This in turn introduces a cost to validating transactions on the ledger—electricity. If operating a mining node and validating transactions were costless, then the network would risk one or more people colluding to operate the number of mining nodes needed to manipulate the ledger—creating millions of virtual nodes. By introducing the concept of scarcity of resources, proof-of-work makes it both technically and economically impractical to control the network in this manner. Although the equipment used to process transactions on the Bitcoin network originally consisted of graphics processing units (GPUs), today there are a number of industrial grade operations leveraging ASIC chips designed specifically for proof-of-work hashing on the Bitcoin network. This has caused some to express concern about the amount of energy expended to maintain consensus across the Bitcoin network and its potentially negative impact on the environment.

Proof-of-Stake

Not all blockchains rely on a proof-of-work consensus algorithm. Instead, some use a technique referred to as "proof-of-stake" or “PoS” to achieve consensus across the network. In a proof-of-stake model, the influence of each node participating in the network is dynamic and constantly adjusted based on its economic stake in the network. There are different methods and mathematical models used to determine the specific methodology used to determine this weighting, but the general idea is to allocate it generally based on the relative loss each node would suffer as a result of a network failure or breach. Economically, this model makes sense from an incentives standpoint—at least on its surface. This assumes, however, that a malicious actor could not easily "short" his position on another exchange in order to profit from a decline in the price of that network's assets. To address this, some models require nodes to post a certain amount of cryptocurrency, in the nature of a bond, in order to ensure their trustworthiness as a validator node on the network.

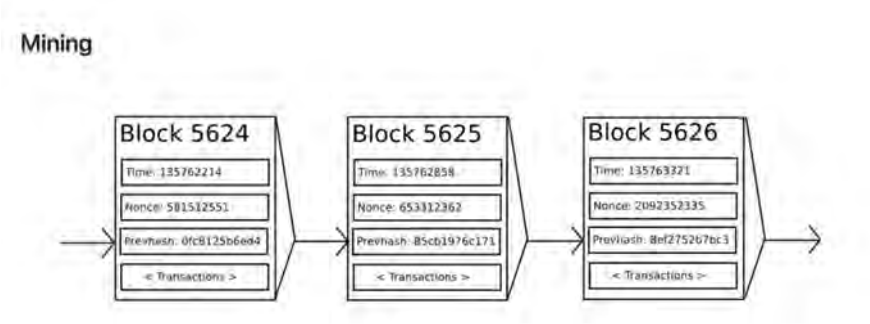


Figure 1. The Ethereum White Paper provides useful depiction of the process of "mining"

BFT

Instead of requiring the use of significant scarce resources, many permissioned protocols rely on Byzantine Fault Tolerance or “BFT” systems, which operate by requiring a certain level of consensus among nodes. If the required number of nodes agree on an update, then it is considered mathematically impossible for someone to have propagated a malicious transaction. Most private consortium ledgers utilize a BFT consensus algorithm. For good reason, many people associate blockchains with PoW, but there are blockchains that use PoS and others that use BFT algorithms. To date, BFT consensus algorithms have almost exclusively been adopted by permissioned networks considered to operate within a “semi-trusted” environment, an assumption that is easier to adopt when the identity of the participants on the network are known to each other. This makes seeking redress from the traditional legal system much more likely than on a pseudo-anonymous public network.

Regardless of the consensus mechanism employed, DLT ledgers are often described as immutable. This perceived immutability is rooted in the acceptance that a properly designed system using one of the above consensus techniques will prevent a malicious actor from altering the records maintained by the ledger. As we will later discuss, sometimes the immutability of a ledger can be challenged by a group of network participants who agree to run a modified version of the protocol software, which results in what is described as a “hard fork”. This phenomenon is not particularly relevant to the protocols likely to be deployed in the loan market—at least initially.

Protocols

Bitcoin

Bitcoin was the first implementation of blockchain technology. The technology and related functionality underpinning bitcoin is sometimes referred to as Blockchain 1.0. Protocols within this category of blockchains, like Bitcoin, are often used to maintain a ledger of all transfers of a native virtual currency. The Bitcoin protocol accomplishes its goal by adding an entry into every ledger connected to the Bitcoin network each time any amount of Bitcoin currency is transferred from one person to another. Units of Bitcoin are stored by reference to public addresses so that anyone can verify that same information. A public address is an alphanumeric string derived from the public key associated with a Bitcoin public key. These keys are generated using public key infrastructure (PKI). The public key can be given out to others and shared freely. The private key, however, must be kept secret. Anything encrypted using the public key can only be decrypted with the private key. A critically important quality, the inability to derive the private key from its corresponding public key and the ability to confirm control over a private key without disclosing it, make it possible to securely create transactions without exposing the private key. Although Bitcoin's importance and its impact on the continued development of DLT cannot be overstated, Bitcoin was not designed to make the loan market operate more efficiently. As such, there is little value in a deeper dive into the intricacies of the Bitcoin protocol.

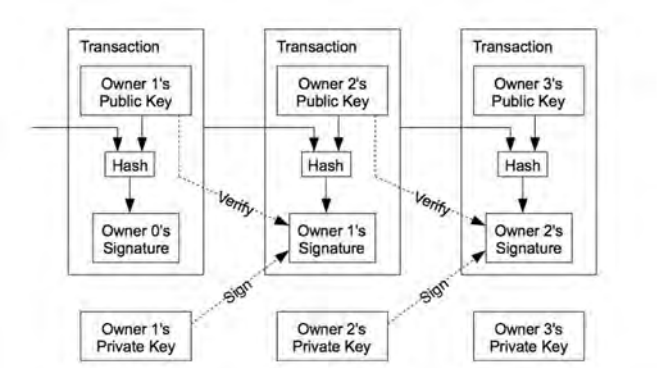


Figure 2. Satoshi's Basic Transaction Design

Ethereum

Although the Bitcoin protocol contains a basic scripting language that allows for some programming functionality, its design is not nearly as robust as the Ethereum Virtual Machine (EVM) that is incorporated into the Ethereum Protocol. The EVM runtime is turing-complete (i.e., a programming language that allows its users to write applications that have no limitations in terms of the logic that can be implemented). The effect of this is to add a fully-functional virtual computer to each node on the network. This improvement to the runtime opened the door to allowing parties to structure and update data on a ledger through robust computer code, known as smart contracts. Instead of a ledger maintaining information about each bitcoin transaction, any asset or thing could be modeled on a ledger. The EVM allows parties to run computer functions to interact with the data structures on the ledger (e.g., transfer, redeem, liquidate, pay etc.). The second part of this paper will dive deeper into the intricacies of smart contracts.

Nevertheless, more robust protocols, such as Ethereum, do not come without risk. In a reminder that blockchain technology is still under development, the DAO (an unfortunate name given it also refers to the concept), an autonomous crowd-funding smart contract, successfully raised over $130 million in Ether (Ethereum's native cryptocurrency). Within just a matter of weeks, however, the DAO was compromised by an individual who was able to find a point of weakness in the smart contract's code and managed to steal $60 million in Ether. The theft raised significant issues about the viability of the Ethereum blockchain network for business use. Ultimately, the

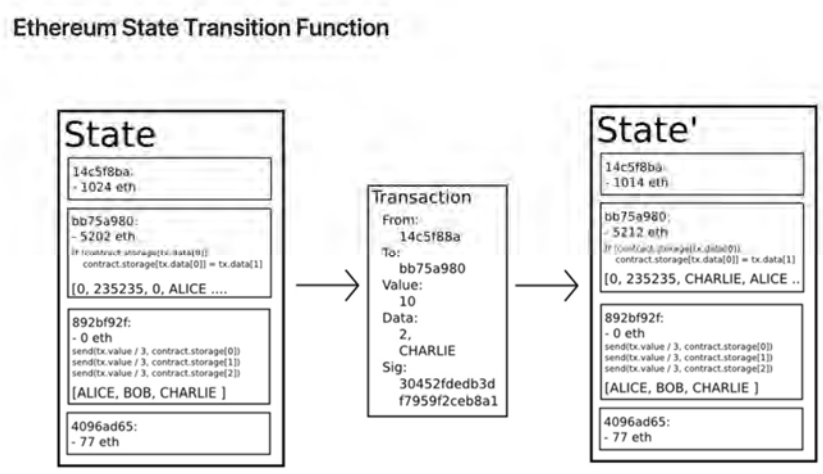


Figure 3. With more functionality comes complexity. (Graphic Ethereum White Paper)

Ethereum community agreed to reverse the transaction that led to the theft (hard fork), which in turn created a new version of the Ethereum blockchain (i.e., a version without the transaction that resulted in the theft). The decision to implement the hard fork was certainly not without controversy, as opponents raged that it contradicted a key tenet (i.e., immutability) of blockchain technology.

Today, several institutions have begun proof of concept projects using private networks running the Ethereum protocol—such as JPMorgan's Quorum. So, although Ethereum was originally designed so that every node within the network executes every smart contract broadcast by any other node, new permissioned versions will permit greater control over who has access to what data on a network. There is significant work underway to incorporate powerful encryption, including zero knowledge proofs, which allow network participants to obfuscate some or all of the data they broadcast on the network.

R3 Corda

R3 has a broad base of US and non-US financial institutions and other diverse participants. Corda is described by R3 as a distributed ledger platform designed from the ground up to record, manage and synchronize financial agreements between regulated financial institutions. Because it was designed for enterprise adoption, specifically finance, Corda is a permissioned system, which grants participants the ability to control access to the ledger. Unlike many traditional blockchains, Corda does not have a native virtual currency, but participants can design and deploy a virtual currency or any other digital model of a real-world asset or entitlement. Like several other protocols, Corda's smart contracts are executed by a virtual machine (the JVM) that is embedded at the protocol level. Although Corda's consensus and validation requirements are different from those of Bitcoin and Ethereum, once consensus is reached, many of the other characteristics discussed above with respect to Bitcoin and Ethereum equally apply. The Corda platform was designed with the heavily regulated environment within which financial institutions operate in mind, which led R3 to incorporate a significant amount of flexibility for users to modify the implementation of the protocol. R3 has successfully developed proof-of-concepts in several types of capital market transactions, including securitizations, supply chain and trade finance and many other use cases. R3 has also

```
public interface ICommercialPaperState extends ContractState {
    ICommercialPaperState withOwner(AbstractParty newOwner);

    ICommercialPaperState withFaceValue(Amount<Issued<Currency>> newFaceValue);

    ICommercialPaperState withMaturityDate(Instant newMaturityDate);
```

Figure 4. Modular approach to contract building. (R3 Project Codebase)

designed Corda for the incorporation of zero knowledge proofs. Ultimately, these and other improvements are leading the way for ever increasingly powerful distributed applications.

Hyperledger Fabric

Like R3's Corda, Hyperledger Fabric is an open source, permissioned protocol. Developed under the umbrella of the Linux Foundation, Hyperledger Fabric is one of several different projects under development under the broader Hyperledger banner. IBM Blockchain is a commercialized version of Hyperledger Fabric offered through IBM's cloud service. Like R3's Corda, network architects have a significant amount of flexibility and the system is designed to be modular (e.g., consensus models are interchangeable). Both R3's Corda and Hyperledger Fabric, because they are permissioned, require one or more certificate authorities to be responsible for issuing digital certificates, and this creates certainty as to the identity of the individuals operating a node or submitting a transaction on the blockchain. Again, this is in contrast to public blockchains like Bitcoin and the public Ethereum network.

Although there are too many protocols, both public and permissioned, to discuss in this paper, the above are a representative sample of different approaches to DLT. In the next part of this White Paper, we consider smart contracts and how their deployment could significantly impact the financial industry.

March 1, 2018

LSTA

White Paper

Blockchain and Distributed Ledger Technology: *An Analysis of its Impact on the Syndicated Loan Market*

Part Two: Smart Contracts

This report was prepared for the LSTA by Holland & Knight LLP.

Introduction to Smart Contracts

Definition and Basic Concepts

The term "smart contract" has been used to describe a variety of concepts (some unrelated to each other), which in turn has led to confusion. One common misconception is that the term "smart contract" is always used to describe a legal contract expressed in the form of computer code[1]. Although it is true that some smart contracts are also legally-binding contracts, the term is also used to describe certain computer code that is unrelated to our traditional notion of contracts.[2] More specifically, within the blockchain community, the term is commonly understood to mean any application code that is designed to automate some business logic within a blockchain or DLT environment. For example, a smart contract might be a simple application that holds virtual currency in a "multi-sig"[3] wallet or even one that runs mathematical operations in

```
pragma solidity ^0.4.8;

import "./Token.sol";

contract StandardToken is Token {
        if (balances[msg.sender] >= _value && _value > 0) {
            balances[msg.sender] -= _value;
            balances[_to] += _value;
            Transfer(msg.sender, _to, _value);
            return true;
        } else { return false; }
    }

    function transferFrom(address _from, address _to, uint256 _value) returns (bool success) {
        if (balances[_from] >= _value && allowed[_from][msg.sender] >= _value && _value > 0) {
            balances[_to] += _value;
            balances[_from] -= _value;
            allowed[_from][msg.sender] -= _value;
            Transfer(_from, _to, _value);
            return true;
        } else { return false; }
    }

    function balanceOf(address _owner) constant returns (uint256 balance) {
        return balances[_owner];
    }

    function approve(address _spender, uint256 _value) returns (bool success) {
        allowed[msg.sender][_spender] = _value;
        Approval(msg.sender, _spender, _value);
        return true;
```

Figure 2 A portion of a standard ERC20 token contract

```
pragma solidity ^0.4.11;

import './ERC20.sol';
import './BasicToken.sol';


contract AccreditationRegistry {
    function get(string _name) constant returns (address);
    function getOrThrow(string _name) constant returns (address);
}


contract Accreditation {
    function isAccredited(address _address) constant returns (bool);
}


contract AccreditedToken is ERC20 {

    AccreditationRegistry accreditationRegistry = AccreditationRegistry(0x0000000000000000);

    bool private registrationStatementFiled = false;

    function getAccreditationStatus() constant returns(address) {
        return accreditationRegistry.getOrThrow("com.hk.token");
    }

    /**
    * @dev Checks modifier and allows transfer if either restrictions turned off or accreditation of propos
    * Otherwise, exit function.
    */
    modifier accreditationVerified(address _to) {
        if (registrationStatementFiled) {
            _;
        } else if (Accreditation(getAccreditationStatus()).isAccredited(_to)) {
            _;
        }
```

Figure 1 A portion of an ERC20 token contract embedding legal logic around transfer restrictions.

[1] Nick Szabo coined the term in 1996, when he published "Smart Contracts: Building Blocks for Digital Free Markets." Szabo's concept of a smart contract was in the context of replacing traditional, paper-based contracts, with digital versions.

[2] In the U.S. there are five (and in some jurisdictions, six) requisite elements of a legally binding contract: (i) offer; (ii) acceptance; (iii) consideration; (iv) mutuality of obligation; (v) competency and capacity; and, in certain circumstances and jurisdictions, (vi) a written instrument.

[3] A multi-sig wallet requires that two or more private keys be used to cryptographically sign a transaction—analogous to a safe deposit box requiring the depositor and the bank to each unlock their respective locks to gain entry to its contents.

exchange for small units of virtual currency. Alternatively, there are smart contracts that do constitute, or implement, legally-enforceable contracts, such as digital bonds, swap instruments and commercial paper, among others; it is this subset of smart contracts that will be the primary focus of this report. [4]

With the incorporation of some of the novel techniques discussed in Part One of this report—mostly inspired by the original Bitcoin protocol—one can create intercompany networks that can automate hundreds or thousands of business and legal processes. This is accomplished by embedding the underlying business and legal logic into a network's implementation software and/or the applications built thereon. The result is a single ledger (*i.e.*, database) that is used by all network participants, across companies, as a single source of truth. Before delving much deeper into the mechanics of how smart contracts work, it is useful to compare the structure (or "stack") of a permissioned[5] DLT-network to those systems upon which our existing business networks are built. As we shall see, many aspects of a DLT-network mirror the architecture of existing software and database structures that have been in use for decades.

In the context of the loan market, let's consider the origination of a syndicated loan on a non-DLT network and a DLT-network. We will assume there is an arranger/administrative agent who extends credit to a borrower (or group of obligors) and other lenders who have received a primary market allocation and will settle those primary trades by funding their pro-rata share of the loan and signing an assignment agreement. If this transaction were closed today, each of the parties involved would be provided with a PDF or another form of the executed credit documents. Each party involved has its own back-office

[4] In the ISDA and Linklaters' Whitepaper titled, "Smart Contracts and Distributed Ledger – A Legal Perspective" dated August 2017, they provide useful definitions for smart legal contracts and smart contract code. The term smart contract is used "to refer to legal contracts, or elements of legal contracts, being represented and executed by software." The term smart contract code "relates less to contracts as a lawyer would understand them, and more to a piece of code (known as a software agent) that is designed to execute certain tasks if pre-defined conditions are met. Such tasks are often embedded within, and performed on, a distributed ledger".

[5] Although much of what follows is equally applicable to public blockchain networks, there are some additional considerations (*e.g.*, game theory) in architecting public networks.

system into which data about the loan must be input. Regardless of the exact system, each will generally consist of one or more user interfaces (a "**UI**") and databases. The application's UI will expose functions allowing a user to create, retrieve, update and delete records ("**CRUD Functions**") in its respective database. Each organization will likely have an access control system ("**ACS**") to limit who can do what with the records in the database—but no one outside of the organization's firewall is intended to have access. After closing, each party will need to manually input the data from its copy of the credit documents into its database system. Thereafter, any modification or other activity affecting the facility will require each of the parties to update and reconcile the records in their respective database. If there are 20 parties involved, then some amendments may require 20 parties to each update their respective database.

On the other hand, a DLT-network running one or more smart contracts can implement identical functionality through a very similar structure and approach, but with one critical enhancement—this database will be replicated across an entire network of computers. Notwithstanding that these computers will be controlled by dozens, or even hundreds, of unrelated parties, the integrity and consistency of the data across the network will be assured by the integration of one of the consensus mechanisms discussed in Part One of this report. In addition, a single ACS, which will now be uniform across the entire network, will control access rights for everyone involved in the transaction. At closing, the credit documents are digitally signed and delivered. As the credit documents are electronically delivered, the deal terms, including information about loan ownership, will automatically populate on the network's ledger. Any subsequent transfers or modifications will require only one update of the ledger, and the system will expose the same CRUD Functions to network participants, with the possible exception of the ability to delete records.

It is tempting to describe the above as nothing more than a distributed database, which would be incorrect. In addition to communicating in a peer-to-peer manner, each node on the network runs an identical virtual environment where code can be executed. This means that when executed, the smart contract will interact with the existing state of the database in a uniform way across the entire network. This shared runtime environment, together with a consensus mechanism to eliminate malicious attempts to manipulate the ledger, create the potential for transformative change in several industries, including finance and the capital markets.

One last general observation about smart contracts. Much has been written about the proliferation of tokens and virtual currency during the last few months. These stories often observe that enterprise systems, like those described above, are separate and distinct from the excitement surrounding Initial Coin Offerings (ICOs). Although there is much truth to the observation, tokens, whether issued in an ICO or as part of an enterprise system, do not really exist beyond the same data entry system described above. In fact, describing digital wallets as being able to "hold tokens" (*e.g.*, this wallet can hold ERC20 compatible tokens) is an abstraction, not a technical description. In reality, a digital wallet holds private keys associated with corresponding public key addresses representing data entries on a ledger. The balance of tokens reflected by a user's wallet is not an indication of anything held by the wallet itself, but rather the value returned by the blockchain's ledger when the wallet retrieved the record storing the balance of tokens. Thus, although the use cases may be different, the underlying technology is fundamentally the same—it's all just a book entry system[6]. We will explore the implications of this next.

[6] This is usually the case with stock certificates and other securities. When a person sells a stock, they are not delivering a physical item to the buyer; instead, they are directing an agent to update their records on who is the beneficial owner of the shares.

Elimination of Reconciliation

The single source of truth that is replicated across the network eliminates the need for parties to reconcile many transactions. In addition, because all the network's nodes can rely on the single source of truth, one can expect a reduction of input errors, litigation and the time it takes each participant to verify whether a party has the claimed rights. Again, this validation is accomplished at the time the entry is made and becomes a part of the ledger, which is trusted on the basis of a consensus algorithm or mechanism. In some markets, like the overnight repo markets, swap markets and other derivatives markets, trillions of dollars in transactions are generated each day. The elimination of reconciliation efforts in these markets would surely reduce transactional costs by billions of dollars every year. What's more, the increased accuracy of records across these markets will lead to a significant reduction in disputes and needless litigation. Many parties are exploring ways to further enhance the integrity of these records through crowdsourcing techniques. Through incentives recorded on the ledger, parties have an economic interest in spotting and reporting errors in any records sent to the ledger. This concept could have sweeping implications for the reference data market and similar information reporting services. One might be inclined to write-off the clearing houses and similar intermediaries as unnecessary in a world driven by DLT, but that would fail to account for the role those institutions play that goes beyond just acting as a settlement agent. It speaks volumes that DTCC is one of the most active companies on Wall Street with respect to DLT research and pilot projects.

Automation

Because smart contracts are, at least partially, self-executing, they require less human interaction and manual processes. This creates an opportunity for better speed, cost and security in the contract lifecycle as compared to traditional contracts. Much of this improvement results from replacing manual

human processes with business and *legal* logic embedded in computer code and deployed on a blockchain. We will discuss certain limitations on transaction throughput later, but many protocols are not able to scale to handle the volume of transactions that existing centralized solutions can process—in some cases, the disparity is dramatic.

Because smart contracts are self-executing, human interaction, and thereby costs, can be reduced from the contract execution, enforcement and reconciliation process. Well-designed smart legal contracts automate onerous administrative tasks associated with contract management such as consents amongst contracting parties, calculating nominal amounts, affirming identification and the transfer of value. A recent Accenture report suggested that US and European banks can save $12 billion annually in operating costs by utilizing smart contracts.[7] Although often overlooked, DLT is one of the most powerful tools for automating businesses and legal processes, maybe even more so than artificial intelligence, including machine learning.

More robust platforms can be designed that trigger automatic payment workflows in fiat currencies (rather than digital cryptocurrencies) by triggering Automated Clearing House (ACH), Swift messages or other payment methods directly from smart contracts implemented on a DLT. Once a transaction is set into motion on a blockchain (*i.e.*, the computer code necessary to provide all information necessary for the transaction is generated and the transaction is "signed" by the pertinent party), it is irreversibly set into motion — no additional wire authorizations, transmissions, deposits, reconciliations, debits and/or credits are necessary. This payment automation can be accomplished without a native virtual currency through the use of a DLT-initiated message that sets the processes into motion on our traditional fiat rails.

[7] Accenture, Banking on Blockchain, https://www.accenture.com/t20171108T095421Z__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Consulting/Accenture-Banking-on-Blockchain.pdf#zoom=50 (2017).

Structuring Smart Contracts

The Relationship between Human Prose and Code

There are different ways of structuring smart contracts. Some approaches include completely replacing traditional (*i.e.*, paper) contracts with smart contracts (*i.e.*, computer code), while others prefer a hybrid approach, combining aspects of traditional contracts with smart contracts. The latter often involves bifurcating contracts into two parts; self-executing and human prose, with the latter (*e.g.*, an arbitration clause) remaining in traditional form and the former (*e.g.*, the transfer of Ether from party A to party B) executed, in code, on a blockchain (this is often referred to as a "Ricardian contract"). For example, if two parties entered into a smart contract to transfer the ownership of a Lamborghini from one party to another, the transfer of payment could automatically (via code) trigger the transfer of Ether from one party to the other upon the smart contract's receipt of notice (from a hypothetical department of motor vehicle oracle) that title to the Lamborghini has transferred to the other party. However, the purchasing party may want to bargain for certain representations, warranties and/or remedies with respect to the vehicle; these provisions (*e.g.*, a representation that the vehicle's manufacturer's warranty is in good standing) may be better addressed in the form of a traditional contract.

Coding and Implementing Smart Contracts

Some or all of every smart contract is embodied in computer code. The type of code depends on the blockchain protocol on which the code is intended to be implemented. For example, a smart contract implemented on the Bitcoin network must be written in Bitcoin's scripting language[8], while a smart contract intended for deployment on Ethereum will most likely be written in Solidity (or possibly Serpent). In the case of Ethereum, the Solidity code will

[8] Practically speaking, Bitcoin's scripting language is too limiting to allow for the development of true smart contracts.

be compiled into byte code (a lower level set of instructions that are machine readable but difficult for humans to understand). This byte code is then executed by the Ethereum Virtual Machine (or EVM), which is the virtual machine running on each node connected to the network. The Fabric implementation of the Hyperledger protocol utilizes the Go programming language[9] to establish the "chain code" which establishes the functionality that will be available on any particular blockchain based on the Fabric protocol. Similarly, smart contracts for R3's Corda are written in either Java or Kotlin and compile to run on the JVM (Java Virtual Machine), which is Corda's virtual machine. Ultimately, the functionality around smart contracts is about implementing CRUD (or more likely, "CRU") operations with respect to data stored in the DLT's ledger. Given one can data model virtually any asset, entitlement, privilege, right or obligation, this is incredibly powerful when coupled with the ability to manipulate the data entries with complex functions.

After determining the conceptual approach that one will take with respect to human prose and code, the next threshold question is what information should exist on the ledger (or "on chain") and what can exist off the ledger (or "off chain"). Putting large documents on chain can potentially slow latency on the network and cause "chain bloat". As such, it's important to be efficient with what is stored across the network. One approach to linking the agreed upon code with a human prose version of the contract is to use a hashing algorithm to create a hash of the final agreement and embed that hash in the smart contract that is deployed to the network. This ensures that only the agreed-upon final contract will match the hash value returned by the hashing algorithm. Given the hash value is only a few characters, it is a fraction of the bytes contained within a 150-page credit agreement.

[9] Although the Javascript based https://hyperledger.github.io/composer/ has gained in popularity.

The Oracle Dilemma

For smart contracts to achieve their full potential, they will likely need to rely on, and respond to, information broadcasted to it from outside sources. These sources of outside information in the blockchain world are often termed "oracles". Oracles introduce a potential threat to the security of smart contracts and thereby the overall transaction; because smart contracts are programmatically designed to self-implement, an erroneous piece of information can irreversibly send a transaction into a tailspin. To illustrate, if, for example, a self-implementing promissory note will need to verify The Wall Street Journal prime rate to determine the interest rate on a variable rate loan, the promissory note (coded as a smart contract on a blockchain) will automatically request an update of the prime rate from The Wall Street Journal. However, if The Wall Street Journal "oracle" is corrupted in any way, the applicable interest rate on the promissory note will be erroneous. The foregoing is a simple illustration of the technologies' need to develop a reliable and robust ecosystem to meet its touted potential.

Proof-of-Stake and Crowdsourcing Data

One approach to the oracle dilemma is to crowdsource the answers or at least verify some other source of the data before the smart contract will execute. If the validators are required to post a stake (usually native virtual currency), resembling a surety bond of sorts, then they will be incentivized to evaluate the data accurately. For those who attempt to input malicious facts around the issue, they will presumably be drowned out by honest responses, in which case their stake is forfeited. These solutions are viable and have tremendous potential. They are, however, complex and rooted in game theory concepts, making them particularly challenging to get right. These solutions are particularly difficult to evaluate for unintended errors given the level of expertise across disciplines required to understand the solutions beyond a surface level comprehension.

Data Security and Privacy

Using a permissioned ledger substantially reduces risks associated with improper or accidental disclosure because accessibility to such ledgers can be specifically controlled. More specifically, protocols such as Hyperledger Fabric and R3's Corda allow participants to control who can see what information about transactions submitted to the ledger. For example, Bank A sells a portion of a syndicated loan to Bank B for $X. Bank A and Bank B can choose to not disclose X to the other participants, even though they are all a part of the permissioned ledger. The ability to maintain an immutable ledger while keeping certain states unknown to unauthorized participants is a critical characteristic of the new wave of DLT.

Because blockchains and distributed ledgers are rooted in asymmetrical cryptography, they are incredibly difficult to defeat through traditional hacking techniques. The actual hacking of the ledger is nearly impossible to do. Like the DAO, however, the biggest concern today is auditing the code that will constitute the smart contract to make sure that it implements the actual intent of the parties. This process requires either a lawyer, who is also capable of reading and understanding the programming language in which the smart contract is written, or alternatively a lawyer and software developer working together to accomplish the same task.

Occasionally, the question is asked about the integrity of DLT in the face of advances in quantum computing. It is true that quantum-based computers, which operate using "entangled particles," could have the computing power necessary to break asymmetrical PKI encryption with brute force. If a DLT solution is built on a modular platform, however, then one can easily swap out an asymmetrical PKI module for an alternative encryption scheme resistant to quantum-based attacks.

Applying Existing Legal Regimes to Smart Contracts

KYC and AML Requirements

An appropriately designed DLT solution would not only meet know your customer (KYC) and anti-money laundering (AML) requirements, but also improve compliance. The LSTA's Guidelines for the Application of Customer Identification Programs, Foreign Correspondent Account Due Diligence, and Other Considerations, dated October 5, 2017, serves as a comprehensive report outlining the specific due diligence and other investigative work that is necessary to engage in primary and secondary market transactions. In order to comply with KYC and AML requirements, any proposed framework should include a secure identity system. This makes a public ledger less desirable as it requires another layer of smart contract implementation surrounding identification. Solutions such as Hyperledger Fabric combine PKI cryptography with a trusted administrator overseeing the membership services component of the platform to ensure that all transactions on the ledger are with known entities.

One significant cost savings from a DLT solution would be an industry-wide reduction in these costs. First, the LSTA's guidelines, which accurately set forth what is required for different transactions and relationships, can be embedded in the smart contract implementing the Framework. This would eliminate transaction delays and inconsistencies in the requirements of similarly situated parties in the marketplace. Second, because the KYC and AML requirements would be incorporated into the Framework, there would no longer be any need to have a separate workflow item for KYC and AML in any syndicated loan market that is processed through the Framework. Given the size of the industry, these savings alone would almost certainly pay for the development and maintenance of a DLT solution.

Electronic Signatures and Enforceability of Smart Contracts and Transferable Records

In addition to Federal legislation commonly referred to as ESIGN, most states have adopted the UETA. The few non-adopting states have nevertheless adopted a statute that deals with electronic records. For example, New York has enacted The Electronic Signatures and Records Act (ESRA). Both UETA and ESRA implement the same public policy as ESIGN by affording electronic signatures the same effect as traditional signatures but without changing substantive law. The goal is to remove barriers to contracting through digital means. Although there are still some documents, such as wills and testamentary trusts, that require an ink signature, none of the exceptions are applicable to the larger capital markets. Because blockchain-based transactions are digitally signed, it is prudent to include a statement of consent to digital signatures in the governance documents.

The UETA also establishes the concept of a transferable record, adopting most of the same language found in ESIGN. UETA's definition of a transferable record is broader in scope in two respects. First, a transferable record can also include an electronic record that would otherwise constitute a document under Article 7 of the Uniform Commercial Code (UCC) if it were in writing. Article 7 of the UCC governs documents of title for personal property. As we will see below in the context of supply chain management, this is important for smart contracts that replace traditional merchant financing that often involve written bills of lading and other forms of documents of title. Again, UETA was adopted well before the development of blockchain technology but nevertheless provides a solid foundation for legally validating smart contracts and the underlying technology itself. Second, a transferable record under the UETA does not need to be secured by an interest in real property, so UETA also encompasses obligations not secured by real property (*i.e.*, obligations secured by personal property and documents of

title).

Cross-Border Issues

Smart contracts raise important jurisdictional questions. Many of these same issues were raised when the internet began to develop, and the world adjusted to a new digital age. Blockchain technology adds an entirely new layer of complexity because of its distributed nature. Unlike a traditional web-based service, there is no central server on which the company does business. Smart contracts work by changing the state of a distributed ledger on every node on the network. In other words, a smart contract is effectively executed on every node across the network (which in the case of Bitcoin or Ethereum means execution across the globe). This means that parties all over the world can easily contract on blockchains running seamlessly in virtually every country. Given this global reach, permissioned ledgers once again eliminate or at least add greater control over managing cross border issues. Although it is possible to address these issues on public ledgers, it is one less issue that needs to be managed.

Antitrust

Companies collaborating with competitors though a blockchain consortium should consider the nature of the information they make available to competitors through a shared ledger. Although certain information sharing is regarded by the antitrust laws to be competitively benign, the exchange of current or future prices or other competitively sensitive information can facilitate price fixing and expose participants to potential antitrust liability.

The appeal of distributed ledger technology lies significantly in the untapped efficiency benefits it offers and not strictly in the opportunities it presents to companies to exchange information, but the technology likely does provide another vehicle that members of a price-fixing cartel could employ to

establish industrywide prices and ensure that members adhere to any agreement. Agreements among competitors related to prices are the most serious of antitrust offenses and can be prosecuted criminally. Participants in blockchain consortia should take care to ensure that they are not, or could not be perceived to be, agreeing to eliminate their independent decision making as to any aspect of the prices they charge. The exchange of specific data on current and future prices and competitive activities – as opposed to aggregated past information – is likely to attract the greatest antitrust scrutiny.

Blockchain consortia will undoubtedly need rules to govern their operations and the interactions of their members. Organizers of these collaborative entities and their participants should consider carefully whether restrictions they impose are necessary to allow the consortia to achieve the promised efficiencies. If they cannot articulate a legitimate basis for any restraints on competition among companies' subject to proposed rules, they should think twice before proceeding with their adoption. Collaborations among users of distributed ledger technology offer to make existing business processes significantly less costly and more efficient. To the extent that the efficiency gains through their collaboration make participation in their consortia essential to the ability to compete meaningfully in the businesses in which the members operate, the members should be aware that they might be required to allow all potential competitors to join the consortia.

There are, of course, potential benefits to regulators arising out of the adoption of DLT systems. Blockchains, by nature, contain a thorough history of essentially all transactions that have taken place on the network, including a time stamp for all such transactions and a consolidated ledger for all transacting parties. These features not only make internal auditing much simpler but also allow for different financial institutions to coordinate their AML efforts in ways that are simply not possible today. By allowing regulators to access the common ledger, they can confirm that all related

transactions are consistent with the stated intentions and information provided by customers. Furthermore, emerging technologies, including the creation of digital identities based on blockchain protocols may not only stymie regulatory concerns with respect to the pseudo-anonymous nature of PKI encryption but may provide a more efficient route to meeting KYC requirements, while continuing to protect the identity of private key holders.

Conclusion

Smart contracts build on the innovation of blockchain technology and have the potential to allow parties to structure and effectuate transactions in a more efficient and secure manner than traditional contracts; however, there are still challenges and obstacles that must be overcome before smart contracts become commonplace. Nevertheless, the technology holds tremendous potential, and when effectively and securely utilized in well-developed use cases, will have a major impact on a number of industries. We will explore some of these challenges and the impact on the loan market in the next part of the White Paper.

April 2, 2018

White Paper

Blockchain and Distributed Ledger Technology: *An Analysis of its Impact on the Syndicated Loan Market*

Part Three: Application of Blockchain Technology to the Loan Market

Table of Contents

Blockchain and the Loan Market

In the first two parts of this white paper, we focused on understanding blockchain and smart contracts more generally. Building on this foundation, this third and final part of our white paper discusses the potential benefits, challenges, and corporate governance issues associated with blockchain and DLT as applied specifically to the loan market. In the past year, several loan market participants have participated in syndicated loan pilot programs designed to leverage blockchain technology. These projects revealed that blockchain has the potential to improve many, if not all, aspects of syndicated lending, including the origination of new loans, the ongoing administration of outstanding loans, and the trading of loans in the secondary loan market.

Potential Benefits of Blockchain

A New Way to Track Ownership: A Single Source of Truth

The loans held by lenders in a syndicate can be tracked automatically on a blockchain platform in the same manner as a cryptocurrency such as Bitcoin is tracked using the same technology. Unlike Bitcoin, however, a blockchain platform for a syndicated loan could also track that loan's interest rate, interest and principal payment dates, and any other data fields relevant to the life cycle of the loan. For example, the data object representing the loan can include fields capable of tracking the borrower's financial reporting requirements and periodic financial covenant testing as required under the terms of the relevant credit agreement, and broadly-supported smart contract standards[1] could make it possible to express those financial covenants in the form of code. In other words, when a borrower periodically submits its financial reports, the relevant financial data could be extracted, and thereafter, that data could be passed to the smart contract, which then uses the agreed formulae (which are coded into the smart contract) to determine automatically whether each covenant is met.

```
1   package loanStruct
2
3   type loan struct {
4       borrowerName    map[string]interface{}
5       adminAgent      string
6       lender          map[string]interface{}
7       loanAmount      int
8       intSpread       int
9       intIndex        int
10      netWorth        int
11      freqTest        int
12  }
13
```

The start of a simple structure for creating data objects representing loans.

At least initially, we expect many lenders in our market to continue to run legacy databases alongside any blockchain platform they implement. Any data on the blockchain's ledger must originate from a machine on which the participant's blockchain protocol software operates and which has access to the necessary private key credentials issued by the blockchain network. In effect, each of these legacy databases will simply be serving as a redundant database and hub that acts as the interface between the ledger and the balance of the institution's systems that are unrelated to the processes that are occurring on the blockchain. As discussed below, having a single source of truth as to the ownership of a syndicated loan ultimately will eliminate the redundant, time-

[1] SWIFT has suggested the use of ISO20022 for distributed ledgers given the number of financial concepts already modeled using this standard. SWIFT. "Business Standards and Emerging Technology." *Information Paper* (2017). For a discussion about the interplay between data objects and structures used by general programming languages (Kotlin, Java, Go, Solidity) compared to extensible markup languages (ISO20022, FpML), see Dewey, Josias N. "Advances in NLP and Machine Learning Justify a New Approach to Smart Legal Documents." *The Third R3 Smart Contract Templates Summit*, New York, New York (2017).

consuming, and costly exercise of multiple parties manually processing and accounting for primary allocations and secondary loan trades.

Elimination of Reconciliation and Reduction of Transactional Costs

Transaction details are stored in structured form in both centralized databases and distributed ledgers. In each case, a well-developed database or distributed ledger will evaluate data entries against certain rules which validate the data (*e.g.*, the sum of each lender's commitments in a revolving credit facility may not exceed the aggregate amount of the commitments of that facility) and will flag "an exception" if a particular rule is not met. For example, a credit agreement may be prepared by legal counsel based on deal terms set out in an email from a client. This approach not only introduces the risk of manual transcription errors, but validation rules are never applied to the information included in the credit agreement.[2] By using document automation tools, together with a distributed ledger, the credit agreement can be generated from validated data stored on the ledger. Although this can, of course, be accomplished without a blockchain, in the absence of a distributed ledger there is no single source of validated data because each lender's data remain behind its own firewall. In a typical syndicated loan, that likely means many different parties, each storing information about a syndicated loan, must continually reconcile all data they receive against their own internal databases. The elimination or significant reduction of reconciliation across the industry and capital markets more generally is perhaps blockchain's most straightforward value proposition for the loan market. As discussed below, there are a number of obstacles that must be overcome before these benefits can be realized.

Improved Regulatory Compliance

Blockchain protocols are generally designed to record a validated history of all transactions that have taken place on the network, including a time stamp for each transaction, all of which are stored as part of a ledger available to all or some network participants. These features not only make internal auditing much simpler, but they may also enable financial institutions to coordinate their anti-money laundering ("**AML**") efforts in ways that are currently difficult to accomplish because of privacy laws. Current blockchain protocols, like R3's Corda and Hyperledger Fabric (these are discussed in Part One of this report), allow for granular control of who can see the different types of data stored on the ledger. This might allow pattern detecting surveillance to pinpoint illicit activities with anonymized data, except that the bank whose customer has been flagged will be identifiable to that bank. Furthermore, emerging technologies, including the creation of digital identities based on blockchain protocols, may not only lessen regulatory concerns with respect to the anonymous and pseudo-anonymous nature of some blockchain protocols but may provide a more efficient route to meeting know your customer ("**KYC**") requirements, while continuing to protect the identity of individuals. One can easily see how such features, if

[2] For an exaggerated example, consider the following set of facts. Bank A originates a $100 million loan to borrower, in which Bank A and Bank B each hold $50 million, while Bank A serves as the agent bank. Bank B's internal systems validate all transaction terms to avoid discrepancies and reduce errors. Bank A doesn't have any such validations. Bank A enters into a trade assigning $30 million to Bank C while purporting to retain $30 million. The trade confirmation and assignment agreement are processed manually by Bank C's loan administration group, who erroneously inputs Bank C's share of the loan as $25 million. After dozens of hours of time are wasted, likely involving loan originators, legal counsel and a host of others, the error will be corrected. Using a blockchain platform, when Bank A inputs the assignment to Bank C, the blockchain will reject it.

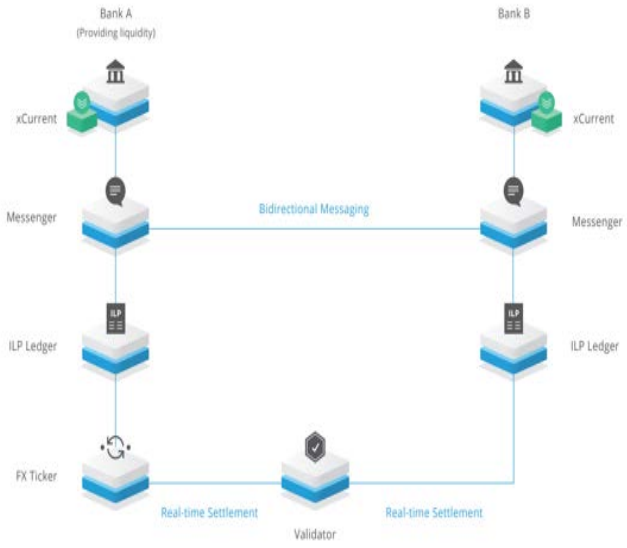
applied to the loan market, could help financial institutions satisfy their AML, KYC, and other regulatory compliance programs.

Authenticity of a Party's Signature

Generally, blockchain transactions must be cryptographically signed by the person in control of the private key; absent that cryptographic signature, the transaction is not valid and will be rejected. This requirement provides strong evidence of authenticity of a person's signature or, at a minimum, that the person who signed had access to the private key. The management of private keys can be challenging, especially at the enterprise level. There are, of course, effective ways to manage private keys, given sufficient consideration and planning. Nonetheless, loan market participants should address the issue as part of the development of any consortium's governance documents, including the risk of loss in the unlikely event of a consensus failure (see discussion below on "**Corporate Governance**").

Use of Off-Chain Processes and Oracles on Semi-Trusted Networks

Secondary market trades in the loan market are memorialized by the parties executing an LSTA trade confirmation. Settlement of the trade—when the seller's legal ownership of the loan is transferred to the purchaser, and the purchaser pays the purchase price to the seller—typically occurs several days or weeks after the trade. Although it seems a forgone conclusion that the adoption of blockchain will shorten the settlement cycle, payment of the purchase price will likely occur outside of blockchain networks for some period of time.[3] As we noted in Part Two, it is not currently possible to transfer U.S. Dollars, Euros, or any other major fiat currency across a distributed ledger.[4] In the future, a central bank issued digital currency could make settlement on the blockchain seamless.[5]



Ripple is building a DLT network of banks, which effectively allows instant, cross-border transfers of fiat currencies.

We previously considered a solution that involved a smart contract triggering an automated series of steps that concludes with fiat currency being transferred across an existing payment solution, such as the United State's

[3] Mills, David et al. "*Distributed ledger technology in payments, clearing, and settlement.*" Finance and Economics Discussion Series. Divisions of Research & Statistics and Monetary Affairs, Federal Reserve Board, Washington, D.C. (2016).

[4] There are some distributed ledger networks that can effectively move fiat currency through partnerships with financial institutions. Ripple, the most well-known of these solutions, is focused on cross border payments.

[5] "[T]he main argument made is that settlement systems for financial transactions could be made more efficient – in terms of operational costs and use of collateral and liquidity – and more secure by using wholesale [Central Bank Digital Currency (CBDC)]. Introducing a wholesale CBDC that is comparable to traditional central bank reserves into interbank payment systems could potentially improve efficiency and risk management in settlement. If complemented by direct participation of non-banks in the settlement process, gains could further increase, including through facilitating the use of new technologies for asset transfers, authentication, record-keeping, data management and risk management." The Committees on Payments and Market Infrastructures, and Markets. "*Central bank digital currencies*." Bank for International Settlements (March 2018).

ACH network, Europe's SWIFT messaging protocol, or other similar "off-chain" funds transfer networks. Using this technique, when the conditions to payment set forth in the smart contract are met, the smart contract will broadcast the occurrence of an "event" that is uniquely associated with a specific transaction. That event will be discoverable by the payor's blockchain node, which, after discovering the event, will delegate the remaining processes off the blockchain. These final processes can still be automated within the payor's internal systems, with the last step being the transmission of electronic payment instructions to the applicable funds transfer network. If desirable, this cycle can be extended by returning a payment confirmation to the blockchain. Because of the difficulty in evaluating and ***trusting*** extrinsic information transmitted to a blockchain,[6] the acknowledgment probably serves little purpose.

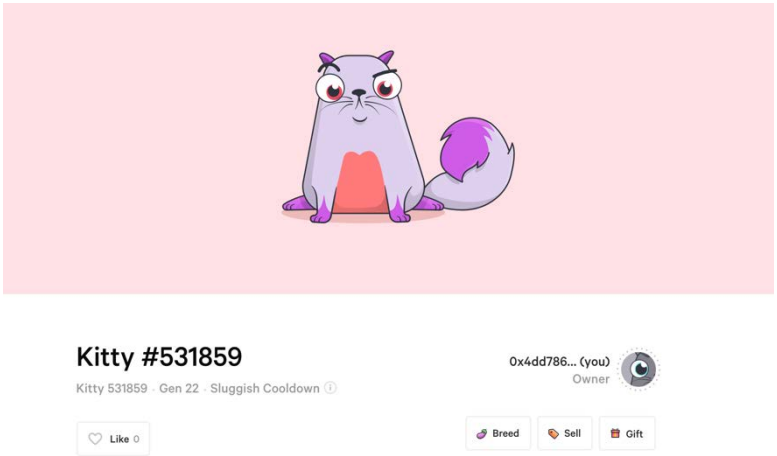
Blockchains are often described as making trust-free commerce possible. This is a fair statement for public blockchain networks, such as Bitcoin and Ethereum; however, permissioned blockchain networks are better described as "semi-trusted" environments because each member of a permissioned network knows the identity of the counterparty on the other side of a transaction. For example, a lender entering a trade to sell its loan will know the identity of the buyer of its loan. Being able to identify a counterparty is important for many reasons, including KYC and AML. For financial transactions, in particular, it provides parties with a way to make formal demand against each other in the event of nonperformance by one of them. Similarly, if the nonperforming party fails to cure the default, the other party may file a lawsuit and exercise its rights and remedies under the transaction documents. By contrast, on public networks, people are often transacting anonymously or with those who have not disclosed their true identity.

This distinction around trust is a critically important one. The method of payment of a purchase price for a loan trade relies on processes external to the blockchain to initiate payment. Reliance on such external processes may be acceptable on a permissioned blockchain network of regulated financial institutions. The introduction of similar external processes on a public network to effectuate settlement might be problematic, and where the identity of the counterparty is not known, simply ill-advised. Consider the example of the person who contracts to buy a digital music library through a smart contract. If the purchase is taking place on a public network, the seller would want the buyer to use virtual currency (*e.g.*, Ether). This would allow the parties to use a smart contract to serve as an intermediary for the transaction. The code will not release the Ether until the digital rights have been transferred to the purchaser, and the code will not release the digital rights until the Ether is released; if the code is written properly, neither party assumes any risk. In contrast, an external payment mechanism provides no such assurance because the payment draft sent to a bank may be declined for insufficient funds. Depending on the composition of the network, this might not be a practical concern for members of a permissioned blockchain network.

[6] See "The Oracle Dilemma" in Part Two of this report.

Challenges to Adoption

Although blockchain technology has the potential to bring about transformative change in the financial markets generally and the loan market specifically, it is difficult to predict when the industry can expect the technology to be implemented in any meaningful way. Arguably, expectations must be tempered and more realistic timelines established. Ironically, for all the talk of transformation, one of the most successful applications of blockchain technology continues to be CryptoKitties[7] - an application that involves the collection, breeding, and trading of digital cats, which managed to draw such an enthusiastic following that it almost brought the Ethereum public network to a grinding halt. If the network struggled to remain functional under the strain of CryptoKitties, questions inevitably arise as to how it would perform under the strain of the global financial markets. Many in the blockchain community chided these digital cats as a frivolous distraction from the serious work of building decentralized applications. Perhaps, however, the naysayers have overlooked the key unintended benefit of this episode, which is to remind us of the challenges and obstacles preventing more widespread adoption of blockchain technology.



A digital cat that lives on a blockchain.

Taxonomy of blockchain's risks.

Number	Risk	Cause	Range of Influence
3.1.1	51% vulnerability	Consensus mechanism	Blockchain1.0, 2.0
3.1.2	Private key security	Public-key encryption scheme	
3.1.3	Criminal activity	Cryptocurrency application	
3.1.4	Double spending	Transaction verification mechanism	
3.1.5	Transaction privacy leakage	Transaction design flaw	
3.2.1	Criminal smart contracts	Smart contract application	Blockchain2.0
3.2.2	Vulnerabilities in smart contract	Program design flaw	
3.2.3	Under-optimized smart contract	Program writing flaw	
3.2.4	Under-priced operations	EVM design flaw	

Blockchain 2.0 introduces new security challenges

Even the best designed blockchain protocol and network are challenging to implement. Careful consideration of countless factors and possible contingencies can mitigate against the risk of technical failures, but it cannot prevent them. Fundamentally, blockchains are complex systems that require different component parts to work seamlessly. Yet, with more robust functionality comes an increased risk of weaknesses around security and system failures.[8] As noted in Part One of this white paper, Bitcoin's success is attributable to its simplicity. Its utility is limited by design in order to keep potential attack vectors to a minimum. As more robust systems are developed, we must respect the fact that systems as complex as these take time to mature; there are no shortcuts.

Nascent Technology

Potential use cases for smart contracts and blockchain technology exist in almost every industry, not just financial

[7] https://www.cryptokitties.co/

[8] X. Li, et al., A Survey on the Security of Blockchain Systems, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2017.08.020.

services. There is, however, a certain amount of hype surrounding some use cases. Although we remain confident that smart contracts and blockchain technology will ultimately transform our market, we recognize that the technology remains in its infancy and is not a panacea for all our market's present challenges. With more time, it will be easier to distinguish between those use cases with real promise and those where existing, traditional, centralized systems function as good as or better than a blockchain would.

Smart contracts are a work in progress, and it will take more time before large segments of our capital markets can depend on them. We cannot lose sight of real life examples of smart contract failures such as the DAO implosion discussed in Part One of this white paper which caused substantial real-world losses. Often times, smart contracts must rely on complex game theory and microeconomic principles to overcome the need for a central figure, intermediary, or other type of traditional centralized system. Writing code with appropriate outcomes and avoiding unintended consequences can be particularly challenging. Lawyers struggle to achieve the same when drafting conventional written contracts, so one can expect coders to struggle with similar issues when trying to embed business and legal logic into their applications. Any solution will, therefore, require a multi-disciplinary approach, drawing on contributions from many fields.

```
1942      /// @notice No tipping!
1943      /// @dev Reject all Ether from being sent here, unless it's from one of the
1944      ///  two auction contracts. (Hopefully, we can prevent user accidents.)
1945      function() external payable {
1946          require(
1947              msg.sender == address(saleAuction) ||
1948              msg.sender == address(siringAuction)
1949          );
1950      }
1951
1952      /// @notice Returns all the relevant information about a specific kitty.
1953      /// @param _id The ID of the kitty of interest.
1954      function getKitty(uint256 _id)
1955          external
1956          view
1957          returns (
1958          bool isGestating,
1959          bool isReady,
1960          uint256 cooldownIndex,
1961          uint256 nextActionAt,
1962          uint256 siringWithId,
1963          uint256 birthTime,
1964          uint256 matronId,
1965          uint256 sireId,
1966          uint256 generation,
1967          uint256 genes
1968      ) {
1969          Kitty storage kit = kitties[_id];
1970
1971          // if this variable is 0 then it's not gestating
1972          isGestating = (kit.siringWithId != 0);
1973          isReady = (kit.cooldownEndBlock <= block.number);
1974          cooldownIndex = uint256(kit.cooldownIndex);
1975          nextActionAt = uint256(kit.cooldownEndBlock);
1976          siringWithId = uint256(kit.siringWithId);
1977          birthTime = uint256(kit.birthTime);
1978          matronId = uint256(kit.matronId);
1979          sireId = uint256(kit.sireId);
1980          generation = uint256(kit.generation);
1981          genes = kit.genes;
```

A portion of the over 2,000 lines of solidity code that make up the smart contract.

In contrast to the DAO's overambitious goals, CryptoKitties is an example of what can be achieved by focusing on incremental improvement. The smart contract for CryptoKitties creates its namesake through the creation of unique digital tokens[9], each of which represents one CryptoKitty. The Ethereum smart contract allows each CryptoKitty to be sold, bred with other digital cats, sired, and have new kittens, all of which involve interaction with the blockchain. The balance of the application, including its user interface, is a traditional web application that interacts with the smart contract through a popular digital wallet[10] installed as a browser extension. The ability to create and administer millions of transferable tokens, each containing unique characteristics, from a single smart contract has relevance to the loan market.

[9] The CryptoKitties smart contract is similar to the popular ERC20 token standard, with one notable exception. The tokens (*i.e.*, the cats) generated by the CryptoKitties smart contract are not fungible. Each CryptoKitty has unique characteristics depending on the composition of its "digital genes". This non-fungible characteristic is implemented by the ERC721token standard, which permits individual tokens to contain metadata that is unique to that token. There are similarities between this and a token representing an interest in a credit facility inasmuch as there may be preferential rights, or the status of the holder was relevant (*e.g.*, a foreign lender).

[10] https://metamask.io/

Given the likelihood that the first blockchain-based syndicated loan platform will be a permissioned blockchain, perhaps like R3's Corda, Hyperledger Fabric (IBM Blockchain) or JPMorgan's Quorum, the abstraction of a

```
pragma solidity ^0.4.11;

-import './ERC20Basic.sol';
 import '../math/SafeMath.sol';

 /**
- * @title Basic token
- * @dev Basic version of StandardToken, with no allowances.
  */
-contract BasicToken is ERC20Basic {
   using SafeMath for uint256;

   mapping(address => uint256) balances;

   /**
-  * @dev transfer token for a specified address
-  * @param _to The address to transfer to.
-  * @param _value The amount to be transferred.
   */
   function transfer(address _to, uint256 _value) returns (bool) {
     balances[msg.sender] = balances[msg.sender].sub(_value);
@@ -27,9 +27,9 @@ contract BasicToken is ERC20Basic {
   }

   /**
-  * @dev Gets the balance of the specified address.
   * @param _owner The address to query the the balance of.
-  * @return An uint256 representing the amount owned by the passed address.
   */
   function balanceOf(address _owner) constant returns (uint256 balance) {
     return balances[_owner];
```

```
pragma solidity ^0.4.11;

+import './LSTABasic.sol';
 import '../math/SafeMath.sol';

 /**
+ * @title Basic registry
+ * @dev Basic version of StandardRegistry, with no allowances.
  */
+contract BasicRegistry is LSTABasic {
   using SafeMath for uint256;

   mapping(address => uint256) balances;

   /**
+  * @dev update registry for a specified address
+  * @param _to The address to which the interest is being assigned.
+  * @param _value The amount of the loan to be transferred.
   */
   function transfer(address _to, uint256 _value) returns (bool) {
     balances[msg.sender] = balances[msg.sender].sub(_value);

   }

   /**
+  * @dev Gets the outstanding balance of the loan for the specified address.
   * @param _owner The address to query the the balance of.
+  * @return An uint256 representing the amount of the loan owned by the passed
+address.
   */
   function balanceOf(address _owner) constant returns (uint256 balance) {
     return balances[_owner];
```

Smart contract, on the left, and the assignment registry, on the right.

"token" will be discarded. Instead, those systems will likely use abstractions, such as an "assignment registry," that is consistent with existing industry nomenclature upon which lenders use private keys digitally to execute LSTA trade confirmations and assignment agreements. When the assigning lender digitally signs the trade confirmation and relevant assignment agreement[11], the registry will be updated to reflect (i) the assignee's account being credited by the amount of the loan transferred to it, and (ii) a corresponding debit to the assignor's account.

The above chart highlights an observation that even those readers with little or no experience with computer programming will likely identify. The only differences between the two snippets of code are those made to the comments describing what the code does. The code itself remains unchanged, as the basic operations needed for either remain the same.

Education

People should understand not only the promise of blockchain, but the challenges to adoption the new technology faces. This suggests that a sustained educational initiative targeting all loan market participants is necessary for the resolution of issues like those discussed in this report, and the LSTA is committed to offering that. It is also important that participants realize that DLT is an evolving technology, and no one can be certain about how exactly it will look in five or ten years. Equally important is that everyone involved realizes that building proof-of-concept systems and even production-ready components (e.g., discrete tasks such as more effective data

[11] If the agent and/or borrower have consent rights, or there are other conditions to the assignment that must be met, the code can be easily modified to incorporate those conditions into the workflow.

management) is part of the education process. In fact, it is more accurate to think of implementing DLT solutions as an evolutionary process, rather than as a traditional system replacement project. So as DLT evolves, so will your DLT implementation and overall strategy.

Interoperability and Industry Support

Perhaps second only to a lack of awareness is the issue of interoperability of systems. Today, we often take for granted the ability of disparate systems to operate and communicate seamlessly. That has not always been the case and still is not completely true in all fields. For example, a large number of traditional database systems store and communicate data in XML schemas, such as SWIFT's ISO20022 and FpML. Blockchain, however, is a relatively new technology in a nascent stage with dozens of different variants being developed (i.e., between permissioned and public ledgers, on-chain and off-chain transactions, basic scripting and Turing-complete programming languages). This disconnect in syntax and protocols can be overcome through the use of application programming interfaces ("**APIs**"), which allow different software applications to speak to each other, even when written in different programming languages. Many APIs that will be needed may already exist, having been developed to permit communication between disparate databases within the same institution.

Forging consensus within an entire industry about standards, best practices, and other uniform approaches and protocols is challenging, as we know. Consensus among participants on technology is only one piece of the blockchain puzzle. There are a number of non-technology matters that must be resolved by participants on any blockchain network. More specifically, matters such as governance, intellectual property, and the actual design and development process should be discussed and agreed and memorialized in writing before too much time is spent on technical evaluation. The LSTA has been following developments around blockchain and providing educational resources to its members for a couple of years and will continue to be a resource as its members navigate many of these challenges and, in some cases, will take a leading role in helping to craft standards that facilitate the efficient deployment of the technology.

Corporate Governance

In this section, we simply seek to highlight some of the issues that should be addressed by a consortium of a group of participants who intend to use a common DLT as the primary instrument for conducting particular transaction types. These are issues which can arise generally within any industry, including our loan market. We would also caution consortium participants about antitrust issues which may arise in such circumstances and to seek advice from counsel where appropriate. Although the task of identifying the correct technology may be challenging, once common ground is reached on that issue, the focus should then turn to internal governance matters and the relative rights and obligations of the participants.

During the process of selecting the appropriate DLT, there will be collaborative efforts necessary to implement the chosen DLT to the specific use case. This collaboration and the development of a technological solution raise intellectual property issues that the parties will want to address. This is especially important if one or more of the participants comes to the table with pre-developed software or other technology. Failure to adequately address these issues could not only risk a party's rights with respect to technology it developed, but also others could find themselves in an unexpected vendor lock-in situation. Although open source is most likely the appropriate route

for many consortia, it may not always be the case, and thus it is important directly to address the issue as part of the governance agreements.

Assuming consensus on the "who" part of the equation is reached, the participants also should address the "how" part as well. Will the development team (which should be a multi-disciplinary group spanning legal, finance, operational, and software development) be in-house members of the participants or will external providers be selected? How will metrics be developed to ensure that project management is effective? How will responsibility be allocated in order to ensure the project doesn't grind to a halt? Once a development team is in place, the consortium can turn its attention to identifying the best architecture that will best serve the consortium. The final architecture will depend, in large part, on the nature of the business logic and process that the consortium intends to implement on the ledger. There are, however, other factors that need to be considered, including regulatory requirements and other requirements imposed on the intended users of the ledger.

After answering all of the above questions, a decision must be made on the means of implementation. For example, a separate corporate body can be formed to oversee the consortium. Alternatively, a trade association could undertake responsibility for the development and/or operation of the DLT consortium. The participants also could choose something short of a separate corporate entity and instead organize as a strategic alliance as evidenced by a separate written agreement. The participants also must address how rules will be changed in the future after the DLT is implemented. Upon the inception of the DLT solution, all participants will operate peer-to-peer nodes that run identical software and smart contracts that embody the DLT solution. At some point, however, whether due to a change in law or market conditions, there will be a need to change one or more of the rules to reflect the business logic in the DLT. How these decisions will be made is something that should be addressed before the DLT is developed, and certainly before it goes online. These efforts are complicated by the ever present need to ensure compliance with applicable antitrust law, an issue that requires continuing diligence and vigilance amongst industry participants.

Conclusion

Although blockchain technology will not eliminate all inefficiencies in the loan market, it seems very likely that blockchain technology will eventually bring about fundamental change in how syndicated loans are originated, administered, and traded in today’s loan market. Yet, there is much work to be done before blockchain is deployed beyond pilots and proof-of-concepts. Computer software engineers, finance professionals, lawyers, and operational personnel will need to work to analyse all of the processes used in the loan market, loan administration, and secondary loan trading. Policy, legal, and regulatory issues will need thoughtfully to be addressed, and we must always balance our desire to promote innovation with the need for a strong, stable, and reliable loan market. It will take time for all of the challenges described in this white paper to be addressed, but, as with the challenges associated with the internet in the 1990s, we are confident they will be overcome.

Consumer Law Meets CYBER LAW

President's Showcase Seminar

SEARCY DENNEY SCAROLA BARNHART & SHIPLEY PA

Attorneys at Law

A Passion for Justice™

Proud to be a sponsor in conjunction with the Consumer Protection Law Committee & The Florida Bar's CLE Committee