NELSON MULLINS

FinTech University
FinTech and eDiscovery

January 10, 2023

Agenda

- FinTech Companies
- eDiscovery Lifecycle
- Information Governance
- Data Preservation
- Messaging Data
- Unique Data Sources
- Apex Discovery
- Sanctions
- Conclusions

FinTech Companies

- What is a FinTech company?
- Startup nature
- Often less history of litigation
- May not have a dedicated legal department
- Unique documents
  - Encrypted emails
  - Prevalence of text/instant messaging
- Unique data types
  - Databases
  - Blockchain
- Greater involvement of c-suite/founders in company operations

eDiscovery Lifecycle

- **Information Governance** – Maintaining policies and procedures designed to mitigate risks and costs associated with electronically stored information ("ESI").
- **Identification** – Locating individuals and data sources likely to maintain potentially responsive ESI.
- **Preservation** – Preventing the loss or alteration of potentially responsive ESI. Required under FRCP 37 and state equivalents.
- **Collection** – Gathering potentially responsive ESI.
- **Processing** – Converting raw data to a reviewable format. Reducing data volumes, including via deduplication and threading.
- **Review** – Identifying documents and information responsive to the request(s). Evaluating responsive documents for privilege, confidentiality, and non-privilege redactions.
- **Analysis** – Identifying key concepts, people, and themes.
- **Production** – Delivering ESI to the requesting party in a useable format.
- **Presentation** – Preparing produced documents and information for use in depositions, interviews, trial, etc.

Information Governance

- Policies and Procedures
  - Bring Your Own Device
    - Who owns the data on the device(s)?
    - What happens when an employee exits the company?
    - Employee privacy concerns
  - Document Retention
    - What categories of documents/information should be retained, for how long, and in what location?
    - Regulatory/statutory obligations
  - Litigation/Preservation Hold
    - When should litigation/preservation holds be issued?
    - Monitoring compliance
- Have policies before you need them!

Duty to Preserve

- Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents. *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003).

- Circumstances that may require suspending normal destruction of electronic information and records include:
  - Actual litigation or arbitration (*e.g.*, lawsuit, subpoena)
  - Government investigation, audit, or other regulatory action
  - Preservation orders issued by the Court in active litigation
  - Notice of a charge or complaint filed with a governmental entity (*e.g.*, EEOC charge, DOL complaint)
  - Lawyer demand letter threatening to sue (depending upon the particular facts and circumstances)
  - Reasonably anticipated litigation
  - A dispute with another party coupled with marking communications about that dispute as "Work Product" or "Prepared in Anticipation of Litigation"
  - An internal investigation or other matter brought to the Legal Department's attention if reasonably likely to lead to litigation or regulatory action

How to Preserve

- Under FRCP 37(e), once the duty to preserve is triggered, a party must take “reasonable steps” to preserve unique, relevant evidence
- The 2015 Amendments to the Federal Rules of Civil Procedure formally added the concept of proportionality to Rule 37
  - As the Advisory Committee comments explain, “The court should be sensitive to party resources; aggressive preservation efforts can be extremely costly, and parties (including governmental parties) may have limited staff and resources to devote to those efforts. A party may act reasonably by choosing a less costly form of information preservation, if it is substantially as effective as more costly forms.”
- Practicality matters – preservation efforts that would cause significant business disruption or require “herculean” efforts are rarely required

How to Preserve (cont.)

- One of the most common steps in preserving ESI is to issue a litigation hold
  - A litigation hold is a notice that informs potential data custodians of their obligation to preserve potentially relevant ESI, identifies the types of ESI that are subject to preservation, and describes how the custodians should comply with their preservation obligations
  - Should be written, not just verbal
  - Issue promptly after the duty to preserve triggers
- Engage custodians to identify potentially relevant sources of ESI for preservation
  - Custodians may have to take affirmative steps to preserve potentially relevant ESI, especially where the ESI is on a mobile device
  - Particularly important when structured data or data in legacy and proprietary systems are involved
- Don't rely solely on custodian self-preservation!
  - Implement back-end solutions if possible, such as by suspending auto-deletion of email
  - Consider whether a custodian may have an incentive to not comply with preservation obligations, such as where the custodian is the subject of an investigation or party to litigation

Messaging Data

- Wide variety of platforms – text message (SMS), iMessage, WhatsApp, Signal, Telegram, Slack, Teams, Discord, and more
- Heavier use by startups and tech companies, especially when significant portions of the workforce are remote or spread across multiple offices
- Preservation, collection, review, and production challenges:
  - Suspend auto-deletion settings on apps and SMS
  - Custodians may not appreciate having their personal messaging data collected
  - Cloud backup vs. full forensic collection of mobile device
  - Messages may span months or years; consider how to separate messages into individual documents
  - Will the produced data look like it did on the app?
- Hot topic for regulators
  - The SEC/CFTC have levied over $1 billion in fines relating to use of personal devices at financial institutions
  - Frequently requested in regulatory investigations

Messaging Data – Recent Case Law

- *Drips Holdings, LLC v. Teledrip LLC*, No. 5:19-CV-02789-JRA, 2022 WL 3282676 (N.D. Ohio Apr. 5, 2022), *report and recommendation adopted in part, rejected in part*, No. 5:19-CV-2789, 2022 WL 4545233 (N.D. Ohio Sept. 29, 2022)
  - Defendant used Slack "as a typical mode of communication for both internal communications as well as customer communications"
  - After duty to preserve had triggered, Defendant changed its Slack retention settings from "indefinite" to seven days and deleted all prior Slack data. Defendant did not revert to indefinite retention for 10 months after receiving a litigation hold notice from opposing counsel.
  - The Court imposed a mandatory adverse-inference instruction for Defendant's spoliation
- *Herzig v. Arkansas Found. for Med. Care, Inc.*, No. 2:18-CV-02101, 2019 WL 2870106 (W.D. Ark. July 3, 2019)
  - After receiving document requests, which covered text/instant messages, Plaintiffs installed Signal on their mobile devices and began communicating solely via Signal
  - Signal is an application allowing users to send and receive encrypted messages, and the Signal messages Plaintiffs sent were not recoverable
  - The Court found that Plaintiffs' use of Signal was a bad-faith attempt to evade document requests

Unique Data Sources

- Databases
  - May contain structured data, which exists in discrete fields (ex., a database showing customer contact information, with fields for name, address, phone number, etc.)
  - Complying with preservation obligations may require taking a snapshot of a system that continually overwrites itself or preserving a backup
  - Consider how best to review and present this information to the judge, jury, or regulator. An expert may be useful in distilling the important pieces of information
  - Legacy systems may pose unique challenges, requiring greater involvement of the company's technical teams
  - "User friendly" databases, like project management programs, can be challenging to produce in a manner that replicates the user experience
- Blockchain Data
  - Generally, there is no obligation to preserve or produce publicly available information
  - Transactions are permanent and immutable, reducing the possibility for discovery disputes about the validity of transaction data
  - Proving ownership of a particular wallet address can be challenging
  - Presenting on-chain transactions to fact finders can require creative thinking

Unique Data Sources – Recent Case Law

- *Famulare v. Gannett Co.*, No. 2:20-CV-13991(WJM), 2022 WL 815818 (D.N.J. Mar. 17, 2022)
  - Defendants used Salesforce to track performance metrics for their account executives, including Plaintiff, a former employee
  - Salesforce displays this information via customizable dashboards, which contain charts, graphs, and other methods of displaying data
  - In response to a request for production of data from Salesforce, Defendant produced "Salesforce's underlying historical data exported to a Microsoft Excel spreadsheet"
  - Plaintiff further requested "reports" showing the dashboards exactly as a user would have seen them
  - Although the parties disagreed over whether generating the reports was technically feasible, the magistrate judge ordered Gannett to at least produce screenshots of the Salesforce dashboard, as that would be the closest to how a user would experience the data in the ordinary course of business

Apex Discovery

- Under the “Apex Doctrine,” courts typically deny attempts to depose senior corporate executives where the apex deponent does not have unique knowledge of the information sought in the deposition or where a lower-level employee has similar knowledge as the apex deponent
- Senior executives of many FinTech companies—especially newer companies—are often involved in meaningful, ground-level decisions, making it difficult to avoid apex depositions or producing the executives’ custodial documents
- Strategies for mitigating the impact of apex discovery
  - Narrow document requests such that senior executives are only custodians for requests for which they contain unique, relevant information
  - Seek protective order to narrowly define the scope of depositions
  - As attorneys, be mindful of executives’ time; gather as much information as possible from other sources, such as lower-level employees and administrative assistants

Potential Pitfalls

- Failure to adequately preserve and produce relevant ESI can have significant consequences
- Monetary sanctions are often awarded where the harm to the opposing party was primarily delay of the litigation and increased discovery expenses related to the misconduct—typically the opposing party's costs in bringing a motion for sanctions
- The worst sanctions under Federal Rule of Civil Procedure 37(e) require that the failure to preserve be "inten[ded] to deprive another party of the information's use in the litigation"
  - Adverse Inference – The fact finder may infer that the lost data would have been damaging to the party that failed to preserve it
  - Default Judgment – In extreme cases, the judge may dismiss the matter (plaintiff misconduct) or enter default judgment (defendant misconduct)
- In government investigations, failure to preserve or produce may lead to reduced cooperation credit or count as an aggravating factor in the event of a settlement

Sanctions – Recent Case Law

- *Red Wolf Energy Trading, LLC v. Bia Cap. Mgmt., LLC*, No. CV 19-10119-MLW, 2022 WL 4112081 (D. Mass. Sept. 8, 2022)
  - Defendants repeatedly failed to produce responsive Slack messages, despite signing multiple affidavits stating that their search was complete, in part due to failure to retain a competent vendor
  - Due to this and other discovery misconduct, the Court ordered default judgment as a sanction
- *Optrics Inc. v. Barracuda Networks Inc.*, No. 17-CV-04977-RS (TSH), 2021 WL 411349, at *4 (N.D. Cal. Feb. 4, 2021)
  - Plaintiff repeatedly failed to meet discovery deadlines and to comply with the Court's discovery orders
  - Plaintiff also failed to issue a litigation hold or to take steps to preserve email or backup desktop computers that likely contained relevant information
  - Plaintiff's employees searched for ESI, especially early in the case, themselves and made responsiveness decisions without fully reviewing documents, often relying on email subject lines
  - The Court imposed approximately $200,000 in monetary sanctions on Plaintiff *and* its counsel, which represented attorneys' fees related to Defendant's response to Plaintiff's discovery misconduct

How to Minimize Risk

- Ignoring the problem won't make it go away and likely will exacerbate it
- The same principles of eDiscovery apply, but with added challenges
- Preparation and policies pay off
- Know your data and systems
- Consult with outside counsel

Presenter Biographies

ROBERT L. LINDHOLM

Rob focuses his practice on government investigations and white collar defense, high stakes business litigation and class action defense, and e-discovery and litigation readiness. He represents companies/individuals involved in the FinTech/Cryptocurrency space (including, among others, Poloniex in its August 2021 settlement with the SEC, various companies/individuals under investigation by U.S. regulators, and Poloniex in the Tether putative class action currently pending in the SDNY), financial institutions, Fortune 500 companies, and other clients in a wide array of internal/government investigations, commercial litigation, and class action litigation. Rob is also the Chair of the White-Collar Crime/Government Investigations Section of the Mecklenburg County Bar.

SOREN YOUNG

Soren practices in the areas of government investigations, class action defense, high-stakes business litigation, and e-discovery and litigation readiness, primarily on behalf of clients in the financial services, pharmaceutical, and FinTech industries, including the emerging cryptocurrency industry. Soren has experience responding to inquiries, enforcement actions, and litigation from the Office of Foreign Assets Control, the Securities and Exchange Commission, the United States Department of Justice, and state attorneys general.

Soren previously worked as an eDiscovery Project Manager for Nelson Mullins's subsidiary Encompass, where he oversaw data collection, document review, and production for matters ranging from hundreds to millions of documents. Soren now serves as national discovery counsel for a Fortune 50 pharmaceutical company. In this role he coordinates discovery for numerous concurrent matters across multiple jurisdictions and before multiple federal regulatory agencies.

Presenter Biographies

RICHARD B. LEVIN

Richard is chair of the FinTech and Regulation Practice and was one of the first lawyers to focus on the regulation of blockchain and digital assets. He is considered a thought leader in the FinTech space. Richard brings his experience as a senior legal and compliance officer on Wall Street and in London to bear in advising clients on corporate, FinTech, securities, and regulatory issues. A problem-solver by nature, he has been advising FinTech clients on legal and regulatory issues since the start of electronic trading in the late 1990s. His practice focuses on helping financial services and technology clients identify and address regulatory issues as they build their businesses.

Richard's practice focuses on the representation of early stage and publicly traded companies in the FinTech space, including investment banks, broker-dealers, investment advisers, peer-to-peer lending platforms, digital currency trading platforms, alternative trading systems (ATSs), exchanges, and custodians. He represents these firms before the U.S. Securities and Exchange Commission (SEC), the U.S. Commodity Futures Trading Commission (CFTC), the Financial Industry Regulatory Authority (FINRA), the U.S. Department of the Treasury, Office of the Comptroller of the Currency (OCC), state regulators, and Congress. Richard has represented clients before regulators in Australia, Canada, France, Germany, Hong Kong, Ireland, Japan, Singapore, South Korea, and the United Kingdom. His current and past clients include leading national financial institutions, multinational financial services holding companies, leading firms in the FinTech space, and institutions engaging in global investment banking, investment management, securities, and other financial services with institutional clients.

Contact Details

To learn more about our FinTech and Regulation practice, or to contact a member of our team, click here or visit our website at nelsonmullins.com.

To learn more about this presentation, please call:

Robert L. Lindholm
301 South College Street
23rd Floor
Charlotte, NC 28202
Tel. 704.417.3231
robert.lindholm@nelsonmullins.com

Soren Young
1320 Main Street
17th Floor
Columbia, SC 29201
Tel. 803.255.9729
soren.young@nelsonmullins.com

Richard B. Levin
1400 Wewatta Street
Suite 500
Denver, CO 80202
Tel. 303.583.9929
richard.levin@nelsonmullins.com

About This Publication

- Nelson Mullins provides this material for informational purposes only.
- The material provided herein is general and is not intended to be legal advice.
- Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations and other legal issues.
- Receipt of this material does not establish an attorney-client relationship.
- Nelson Mullins is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements.