November 4, 2022

From Cyber Crisis to Courtroom

Mitigating Litigation Risk and Liability Exposure in the Incident Response Process

Ed McAndrew
BakerHostetler

James Perry
CrowdStrike

Nate Lovett
Wiley Rein LLP

Privacy+ Security Forum

Speakers

Privacy+ Security Forum

Ed McAndrew

Partner,
Cybersecurity &
Litigation
BakerHostetler

Nate Lovett

Associate
Insurance & Privacy,
Cyber & Data
Governance
Wiley Rein LLP

James Perry

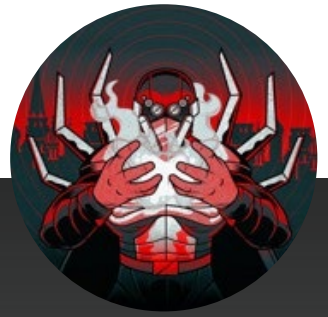
Senior Director of
Consulting Services
CrowdStrike

A Changing Threat Landscape

Privacy+ Security Forum

The threat landscape is evolving






- Threat landscape is accelerating
- Proliferation of sophisticated threat actors across the globe (185 tracked)
- Increase in identity-based attacks
- Nation States focus on stealing credentials and using those to access data
- May groups have evolved to data extortion

How adversaries gain access:

- Valid credentials
- Supply chain attacks
- Zero day exploits
- MFA bypass

How adversaries remain stealthy:

- Living off the land

What adversaries are attacking:

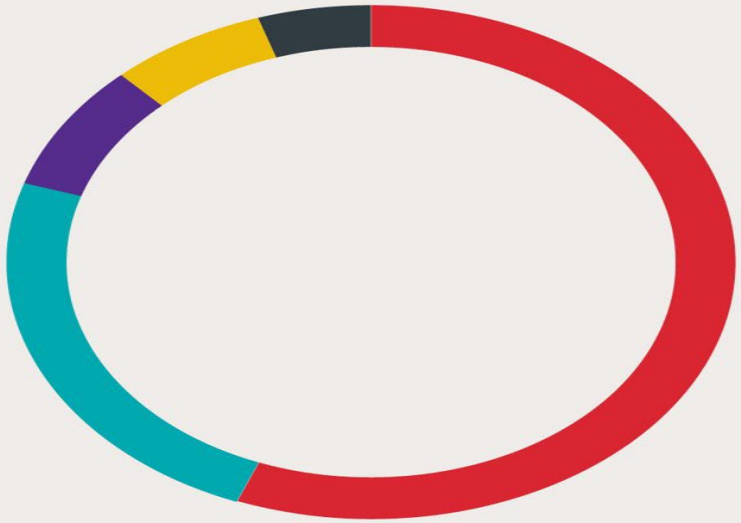
- Cloud workloads
- Email servers
- Downstream access

2022 BakerHostetler DSIR

Attack Types

Privacy+ Security Forum

Top 5 Causes



56% Network Intrusion

24% Phishing

8% Inadvertent Disclosure

7% System Misconfiguration/ Accessible Cloud Asset

5% Stolen/Lost Devices or Records

What Happens Next

37% Ransomware

27% Theft of Data

21% Office 365 Account Access

17% Installation of Malware

10% Wire Transfer

2% Cryptomining

1% Espionage

2022 BakerHostetler DSIR

Response Timelines

Privacy+ Security Forum

Detection

Occurrence to Discovery

MEDIAN

13 Days

AVERAGE

ALL INCIDENTS
84 Days

NETWORK INTRUSION
66 Days

Containment

Discovery to Containment

MEDIAN

0 Days

AVERAGE

ALL INCIDENTS
5 Days

NETWORK INTRUSION
4 Days

Analysis

Time to Complete Forensic Investigation

MEDIAN

30 Days

AVERAGE

ALL INCIDENTS
38 Days

NETWORK INTRUSION
41 Days

Notification

Discovery to Notification

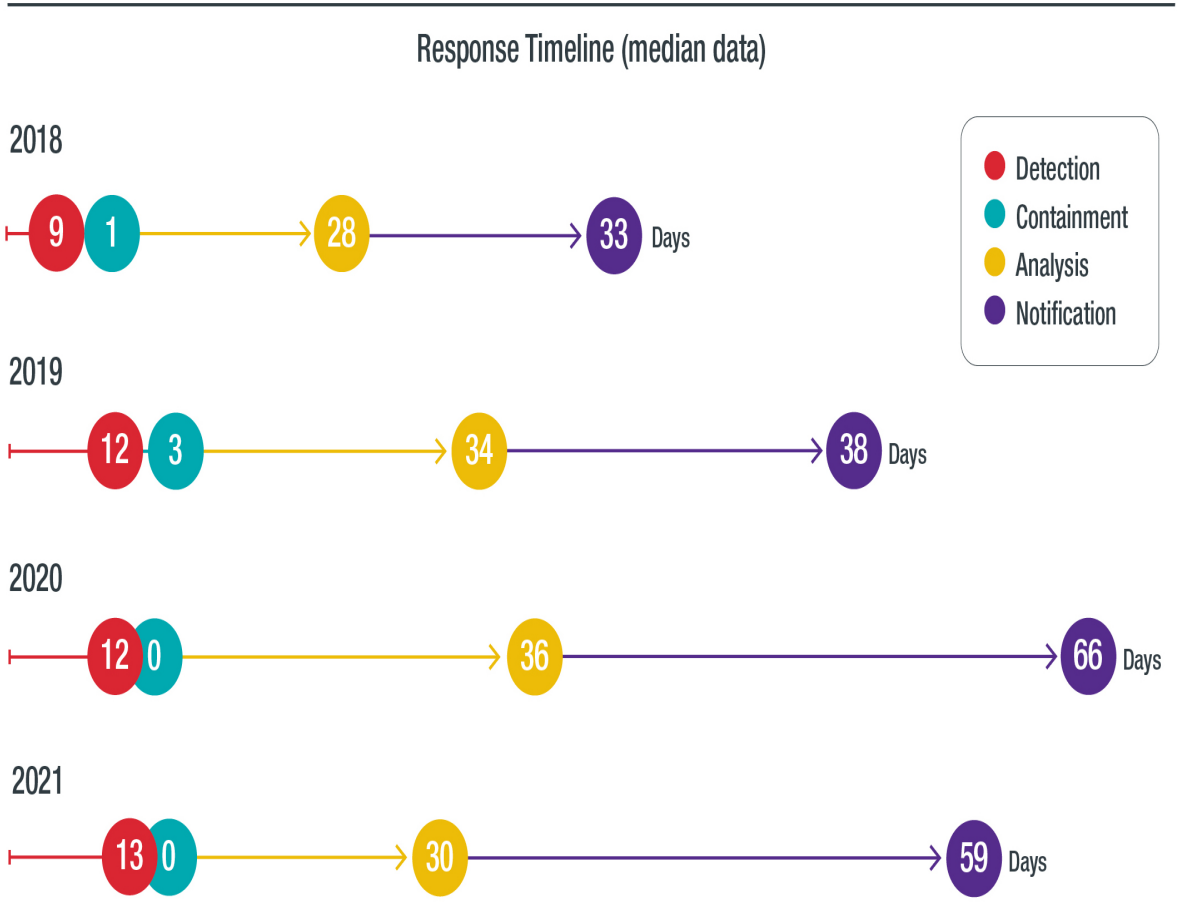
MEDIAN

59 Days

AVERAGE

ALL INCIDENTS
74 Days

NETWORK INTRUSION
72 Days



2022 BakerHostetler DSIR

Forensics v. Legal Exposure

Privacy+ Security Forum

Average Forensic Investigation Costs

$56,728 All Incidents

$74,554 Network Intrusion Incidents

$445,926 20 Largest Network Intrusion Incidents

Regulatory Inquiries Following Notification

Notifications vs. Lawsuits Filed

536 Notifications

23 Incidents Resulted in Lawsuits

2022 BakerHostetler DSIR

Incident-related Class Actions

Privacy+ Security Forum

23 incidents disclosed in 2021 resulted in one or more lawsuits filed (compared to 20 in 2020).

- **19** incidents involved SSNs
- **16** incidents involved medical/health information
- **5** incidents involved payment card data
- **3** incidents started with system misconfiguration
- **15** incidents involved ransomware
- **18** incidents started with network intrusion
- **4** incidents were vendor related

58+ total lawsuits filed related to the 23 incidents

- **8** incidents had more than one (but less than 5) lawsuits filed
- **4** incidents had five or more lawsuits filed
- **43** lawsuits were against a healthcare organization

Number of Incidents that Resulted in Lawsuits by Individuals Notified

8	11	3
over 1.2 million	under 700,000	under 8,000

2022 BakerHostetler DSIR

Ransomware/Cyber Extortion

Privacy+ Security Forum

80% of the time an organization was able to partially or fully restore from backup without paying ransom

82% of ransom notes contained claim of theft of data before encryption

73% found evidence of data exfiltration when there was a claim of data theft in the ransom note

$60+ million
Largest ransom demand in 2021
(2020 was $65+ million)

$5.5 million
Largest ransom paid in 2021
(one variant was involved in six of the 10 largest 2021 payments)

$511,957
Average ransom paid in 2021
(2020 was $794,620)

11.1 Days
From demand to payment (median: 8)

9.8 Days
From demand to payment for payments over $1 million (median: 8)

13 Days
From demand to payment for payments $200,000–$1 million (median: 10)

12.2 Days
From encryption to restoration (median: 9)

81% involved theft of data resulting in notice to individuals

24% of matters involved a payment to a threat actor group even though the organization had fully restored from backup

33% paid even though the organization was able to partially restore from backups

37% of total matters involved ransomware

35% of healthcare matters involved ransomware

2022 BakerHostetler DSIR

Ransomware/Cyber Extortion

Average Ransom Paid

$511,957

AVERAGE

	INITIAL RANSOM DEMAND	RANSOM PAID	DAYS TO ACCEPTABLE RESTORATION	FORENSIC INVESTIGATION COST	INDIVIDUALS NOTIFIED
Healthcare	$8,329,520 (median: $1,043,480)	$875,784 (median: $500,846)	6.1 (median: 0)	$62,724 (median: $28,000)	81,679 (median: 1,002)
Financial Services	$3,064,559 (median: $1,000,000)	$513,928 (median: $250,000)	12.8 (median: 5)	$39,380 (median: $15,000)	64,795 (median: 837)
Retail, Restaurant, & Hospitality	$3,032,936 (median: $1,100,000)	$351,986 (median: $137,500)	7.8 (median: 7)	$90,192 (median: $46,625)	85,036 (median: 456)
Manufacturing	$2,362,636 (median: $1,000,000)	$593,993 (median: $283,500)	10.2 (median: 5)	$49,304 (median: $32,000)	1,854 (median: 784)
Education	$1,588,468 (median: $558,000)	$196,071 (median: $154,000)	10.5 (median: 8)	$68,729 (median: $47,520)	14,168 (median: 1,268)
Business & Professional Services	$1,383,704 (median: $409,800)	$342,370 (median: $120,892)	10.8 (median: 7)	$42,815 (median: $27,102)	9,131 (median: 361)
Energy & Technology	$9,553,333 (median: $10,400,000)	$3,000,000 (median: $2,000,000)	4.6 (median: 2)	$99,358 (median: $53,000)	21,096 (median: 426)
Government	$764,500 (median: $450,000)	$142,122 (median: $105,000)	11.5 (median: 10)	$44,704 (median: $36,500)	12,985 (median: 174)

2022 BakerHostetler DSIR

Vendor-related Incidents

Privacy+ Security Forum

19% of total incidents involved vendor causes

55% of vendor-caused incidents had notice requirements

10% of notices had regulatory inquiries

Discovery and Notification Timelines Vary Greatly The time it takes vendors to notify their customers of an incident can vary greatly depending on the type and extent of the incident, the scope of the vendor's services, and the parties' legal or regulatory obligations. This often leads to a longer notice timeline to individuals.

Information Sharing Also Varies Because the incident occurred at the vendor, the vendor controls the investigation, as well as what information is shared with customers and when. Even after completion of the investigation, vendors may be unwilling to share full details, which is often frustrating to customers.

Vendor Vetting (and Re-Vetting) Remains Key Before engaging a new vendor that will receive access to their environment or data, customers must exercise due diligence to make sure the vendor has adequate security safeguards in place. Ongoing vendor diligence is also critical to help prevent an incident involving their data.

Understand and Limit Data Sharing On both the customer and vendor side, minimizing the personal and/or sensitive information shared with or accessed by a vendor can mitigate risk and exposure.

Make Notice Provisions Make Sense Customers often try to add urgency to vendor breach notification obligations through contract language (e.g., "immediately," "within 24 hours," "within 72 hours"). However, as incident responders know, upon discovery, there is little meaningful information available, and downstream contracts are often not top of mind. It's important to strike a balance between a desire for transparency and the realities of breach response to ensure the notice customers receive is useful and actionable. This is especially important for highly regulated organizations, like healthcare providers and financial institutions, as vendor incident notifications could "start the clock" on their legal breach notification deadlines, which could be problematic if the scope of the incident and data involved is not yet known.

Know Your Remedies When an incident involves thousands of customers, the language in the vendor contract is critical to determining customers' rights.

Customers Face Regulatory Scrutiny and Class Actions Too Despite incidents occurring at the vendor, we do see regulatory investigations and class actions against downstream customers.

2022 BakerHostetler DSIR

BECs/Financial Fraud

Privacy+ Security Forum

$48 million
In fraudulent wire transfers

$743,106
Average wire transfer

$166,257
Median wire transfer

$12 million
Largest wire transfer

$10.2 million
Second-largest wire transfer

$890,135
Average recovery

$181,577
Median recovery

43%
Matters that had recovered funds (totaling over $24 million combined)

- Greater Use of Stolen Data from Ransomware Attacks to Commit Fraud
- Pivot to Financial Fraud for "Easy Money"
- Remote Work Vulnerabilities
- More Fund Transfer Incidents Are Triggering Legal Notification Obligations
- Recovery Rate Is Increasing Where Re-direction Is Spotted Quickly

These steps may help your company prevent fraudulent transfer incidents:

1. **Use MFA** for remote access to online accounts, including email and payroll portals, and disable legacy authentication in your email tenant.
2. **Train employees** regarding phishing emails and common fraudulent fund transfer schemes.
3. **Establish written policies and procedures** related to authorization and approval of changes to wire transfer, ACH payment, and direct deposit information.
4. **Design contract provisions** with vendors and customers that require in-person or voice authentication for changes to existing wire transfer, ACH payment, and direct deposit information.
5. **Research** if something seems awry, look up the telephone number that you have on file for the email sender (not the contact listed in their email), and call the sender to confirm that what is being requested is legitimate.

Key Issues in Incident Response

Privacy+ Security Forum

Cyber Extortion

Privacy+ Security Forum

Detection, Containment and Team Scaling	Remediation Planning – operationally down, extortion	Crisis Management and Communications	Threat Actor Engagement and Ransom Negotiation
OFAC and Law Enforcement Issues	Insurance support, Documentation support from vendor	Legal Disclosure Obligations	Litigation Planning

Cyber Extortion

Threat Actor Engagement

Privacy+ Security Forum

- ✓ **May be essential to buy time**
  - ✓ Can you restore operations before “time expires”?
  - ✓ How much time do you need to (1) determine the full scope and potential consequences of the incident; and (2) execute workstreams to mitigate negative consequences?
- ✓ **Key issues to consider**
  - ✓ What key factors should we consider in determining whether, when, and how to engage the threat actors/possibly pay a ransom?
  - ✓ Is it legal to communicate with a threat actor? Is it legal to pay a ransom? Under what circumstances?
  - ✓ How would we handle communications with threat actors?
  - ✓ How would we execute the negotiation and payment of a ransom?
- ✓ **Engage experienced ransomware negotiation consultant through counsel**
  - ✓ Maintains Attorney-Client Privilege and Work Product Protection
  - ✓ Early engagement is needed to stall additional threat actor malign activity or to cut a quick deal where prudent.
  - ✓ A specialist ransomware consultant can assist with:
    - ✓ Validating the credibility of the attack and potential impact of future actions
    - ✓ Providing intelligence about the motives and temperament of the attackers
    - ✓ Negotiation strategy and tactics – art informed by intel
    - ✓ Accessing crypto and facilitating LEGAL payment
    - ✓ Executing decryption process/data impact analysis
  - ✓ Specialists provide OFAC compliance reports and a chat transcript that will not be needlessly damaging in ensuing investigations or litigation.

Cyber Extortion

OFAC Ransomware Guidance

- IEEPA/TWEA -- U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria).
- OFAC may impose civil penalties for sanctions violations based on strict liability.
- DOJ may prosecute willful violations of IEEPA/TWEA
  - IEEPA – willfully attempting, conspiring, causing or violating any license, order, regulation or prohibition issued under the statute.
  - TWEA – willfully violating any provision of TWEA or any license, rule, order or regulation issued thereunder.

DEPARTMENT OF THE TREASURY

Office of Foreign Assets Control

31 CFR Part 578

Cyber-Related Sanctions Regulations

AGENCY: Office of Foreign Assets Control, Treasury.

ACTION: Final rule.

SUMMARY: The Department of the Treasury's Office of Foreign Assets Control (OFAC) is amending the Cyber-Related Sanctions Regulations and reissuing them in their entirety to further implement an April 1, 2015 cyber-related Executive order, as amended by a December 28, 2016 cyber-related Executive order, as well as certain provisions of the Countering America's Adversaries Through Sanctions Act. This final rule replaces the regulations that were published in abbreviated form on December 31, 2015,

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments[1]

Date: September 21, 2021

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this updated advisory to highlight the sanctions risks associated with ransomware payments in connection with malicious cyber-enabled activities and the proactive steps companies can take to mitigate such risks, including actions that OFAC would consider to be "mitigating factors" in any related enforcement action.[2]

Demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations. The U.S. government strongly discourages all private companies and citizens from paying ransom or extortion demands and recommends focusing on strengthening defensive and resilience measures to prevent and protect against ransomware attacks.

OFAC Ransomware Guidance

General Factors Affecting Administrative Action -- 31 C.F.R. Pt. 501 App. A, § III

Privacy+ Security Forum

- Willful or Reckless Conduct (knowledge of violation of US law/failure to exercise minimal degree of caution/care, disregard for warning signs)
- Concealment (hiding conduct to mislead OFAC, federal, state or foreign regulators or other involved parties)
- Pattern of Conduct (pattern or isolated/atypical occurrence)
- Prior Notice (reasonably on notice that conduct was illegal)
- Management Involvement (D&O, supervisory or managerial staff aware or should have been aware)
- Awareness of Conduct (greater the actual knowledge, greater the penalty)
- Harm to Sanctions Program Objectives (benefit to sanctioned person/entity; impact on US policy; license eligibility; humanitarian activity)
- Individual Characteristics (commercial sophistication, operational size and financial condition, transaction volume, sanctions history, compliance program, voluntary corrective action)
- Cooperation with OFAC (voluntary self-disclosure, production of all relevant information, SOL tolling)

OFAC Ransomware Guidance

Sanctions Compliance Program and Defensive Resilient Measures

Privacy+ Security Forum

- "[t]he existence, nature and adequacy of a sanctions compliance program is a factor" in OFAC enforcement determinations.
  - Implementation of a risk-based compliance program mitigates exposure to sanctions-related violations.
  - Integrate ransomware response activities into existing compliance programs.
- Adoption and improvement of cybersecurity practices "will be considered a significant mitigating factor in any OFAC enforcement response.
  - See CISA September 2020 Ransomware Guide
  - Key steps highlighted in OFAC Guidance:
    - Offline data backups
    - Incident response planning
    - Cybersecurity training
    - AV/Anti-Malware updating and software patching
    - Authentication protocols and access management (MFA, etc.)
- "OFAC will consider a Company's self-initiated and complete report of a ransomware attack to law enforcement or other relevant U.S. government agencies . . . made as soon as possible after discovery of an attack . . . to be a voluntary self-disclosure and a significant mitigating factor"
  - "OFAC will also consider a company's full and ongoing cooperation with law enforcement both during and after a ransomware attack – e.g., providing all relevant information such as technical details, ransom payment demand, and ransom payment instructions as soon as possible – to be a significant mitigating factor."
- Following the steps above would make it more likely that OFAC would resolve sanctions violations with a non-public response.

Privilege in Investigations

Privacy+ Security Forum

Legal Privilege in the United States

BakerHostetler

- *Applicable privileges can arise under state or federal law. The three primary "privileges" that arise in cyber incident investigations are:*

1. Attorney-Client Privilege

- A state and federal common law privilege that protects confidential communications between attorney and client for the purpose of seeking and providing legal advice.
- It may encompass non-lawyer agents working at the direction of counsel for the purpose of assisting counsel in providing legal advice.

2. Work Product Doctrine

- A qualified immunity protecting from discovery documents and tangible things prepared by a party or its representative in anticipation of litigation or for trial.
- Creates a presumption against discoverability that may be overcome on a showing of compelling need (for attorney's mental impressions and opinions) or substantial need (for non-opinion work product).

3. Common Interest Doctrine

- Confidential communications between multiple parties shared to advance a claim or defence remain privileged.
- This may apply to communications with third party service providers of the company suffering the incident.

Sampling of Key Decisions on Legal Privilege

Privacy+ Security Forum

- **Incident Response Materials Protected by Privilege**
  - *In re Marriott int'l Inc. Customer Data Sec. Breach Litig.*, 2021 WL 2910541 (D. Md. July 12, 2021)
  - *In re Capital One Consumer Data Sec. Breach Litig.*, 2020 WL 5016930 (E.D. Va. Aug. 21, 2020) (denying mot. Compel PwC Rpt withheld on privilege)
  - *In re Target Corp. Customer Data Sec'y Breach Litig.*, 2015 WL 6777384 (D. Minn.)
  - *In re Premera Blue Cross Customer Data Sec'y Breach Litig.*, 329 F.R.D. 656 (D. Or. 2019)
  - *In re Experian Data Breach Litig.*, 2017 WL 4325583 (C.D. Cal. May 18, 2017)
- **Incident Response Materials NOT Protected by Privilege**
  - *In re Rutter's Data Sec. Breach Litig.*, 2021 WL 3733137 (M.D. Pa. July 22, 2021)
  - *Wengui v. Clark Hill, PLC*, slip op. (D. D.C. Jan. 12, 2021)
  - *In re Capital One Consumer Data Sec. Breach Litig.*, 2020 WL 2731238 (E.D. Va. May 26, 2020), *aff'd* 2020 WL 3470261 (E.D. Va. June 25, 2020) (granting mot. compel production of Mandiant Rpt)
  - *In re Dominion Dental Servs. Data Breach Litig.*, 429 F. Supp. 3d 190 (E.D. Va. 2019)
  - *In re Premera Blue Cross Customer Data Sec'y Breach Litig.*, 296 F. Supp. 3d 1230 (D. Or. 2017)
- **Waiver of Attorney-Client Privilege**
  - *In re United Shore Fin. Servs.*, 2018 WL 2283893 (6th Cir. Jan. 3, 2018)
  - *In re Target*, 2015 WL 6777384 (D. Minn.)
- **Work Product**
  - *Commonwealth v. Equifax*, 35 Mass. L. Rptr. 416 (Mass. Super. 2018)

Regulatory Investigations & Civil Litigation

Privacy+ Security Forum

Legal Obligations and Impact on Strategy

What is the potential regulatory or civil liability as a result of disclosures and the incident itself?

- Negligence
- Negligence Per Se
- Negligent Failure to Warn
- Breach of Contract/Implied Contract
- Violation of federal/state privacy and information security statutes
- Violation of Breach Notification Statutes
- Unfair Trade Practices/Consumer Fraud
- Fraudulent Misrepresentation

What is the potential for involvement in criminal or other proceedings as a result of the incident?

Data Security and Data Breach Notification Laws

Privacy+ Security Forum

DATA SECURITY LAWS

- 26 states have enacted general data security laws
- 18 states have adopted a version of the NAIC Model Insurance Data Security Act
- Data security laws generally require businesses to:
  - Maintain appropriate security policies, procedures and safeguards (encryption, least privilege, multi-factor authentication)
  - Appoint a cybersecurity leader
  - Create an Incident Response Plan
  - Train employees
  - Oversee service providers
  - Periodically assess risks
  - Monitor their programs
  - Fund their programs
  - Maintain Board Oversight

DATA BREACH NOTIFICATION LAWS

- 50 State laws & Numerous Federal Laws
- "Personal Information" definitions are expanding
- Regulator notification expanding – 37 states
- Notification timeframes are tightening
  - SEC Proposed Rule – 4 days
  - FFIEC Proposed Rule – 36 hours
  - NY DFS Cybersecurity Regulation and SHIELD Act – 72 hours
  - GDPR – 72 hours
  - State laws – as expeditiously as possible
  - Contracts/Outside Counsel Guidelines – immediately/24 hrs
- Litigation is growing as cases survive early dismissal
  - Consumer Privacy Class Actions
  - Regulatory Enforcement Actions
  - Shareholder/D&O
  - Commercial and Employment Litigation
  - Insurance Coverage

Statutory Private Causes of Action for Cyber Incidents

Privacy+ Security Forum

California Consumer Privacy Act -- Cal. Civ. Code § 1798.150(a)(1)

Private Cause of Action

"Any consumer whose nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action . . . ."

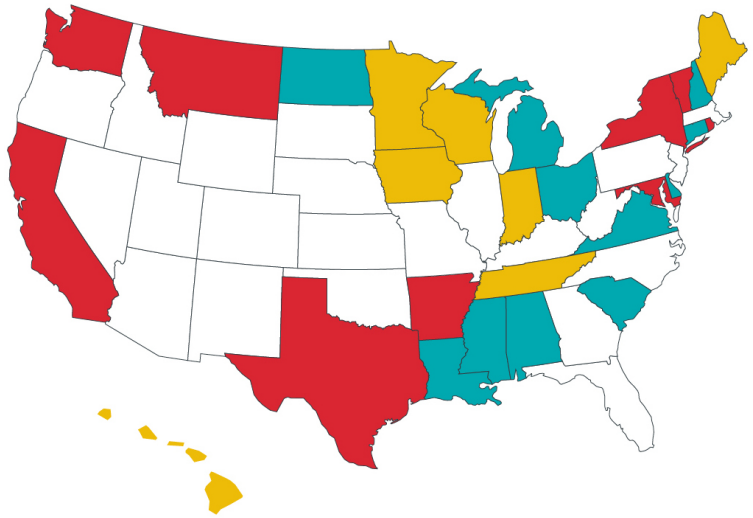
Statutory Damages

- Statutory damages of **at least $100 and up to $750 per consumer, per data breach** for a breach of unencrypted/unredacted personal information resulting from a business's failure to implement reasonable security measures.
- Court may also award actual damages (if greater than statutory damages), injunctive or other relief.
- Damage assessment considers, among other factors: nature, seriousness, persistence and duration of misconduct; number of violations; willfulness of the business's misconduct; business's assets, liabilities and net worth.

Other States Permit Recovery of Treble Damages and Attorney's Fees for gross negligence or willful misconduct.

Recent Insurance Sector Laws

Privacy+ Security Forum



Newly adopted laws based on NAIC Model Law

Hawaii, Indiana, Iowa, Maine, Minnesota, Tennessee, Wisconsin

Previously enacted laws based on NAIC Model Law

Alabama, Connecticut, Delaware, Louisiana, Michigan, Mississippi, New Hampshire, North Dakota (WISP requirements effective 8.1.22), **Ohio, South Carolina, Virginia** (WISP requirements effective 7.1.22)

Enacted laws or provided guidance not based on NAIC Model Law

Arkansas, California, Maryland, Montana, New York, Rhode Island, Texas, Vermont, Washington

A Tort Duty to Safeguard Personal Data

Privacy+ Security Forum

- *Dittman v. UPMC* (Pa. S. Ct. Nov. 21, 2018)
  - Arose out of data breach impacting personal information of all employees.
  - Reversed dismissal of data breach class action.
  - An employer that collects personal information from employees has a common law duty to exercise reasonable care in securing that information against foreseeable cybersecurity risks.
  - The economic loss doctrine does not prevent the recovery of purely economic damages for a data breach under a negligence theory.
  - Broad rationale easily expandable to all data collectors.

- *In re Rutter's Inc. Data Security Litig.*, slip op. (M.D. Pa. Jan. 5, 2021)
  - Denying motion to dismiss negligence claim in consumer data breach class action
  - Extending rationale of *Dittman* to customer bank card data

Damages Can Vary Widely in Cyber Incident Litigation

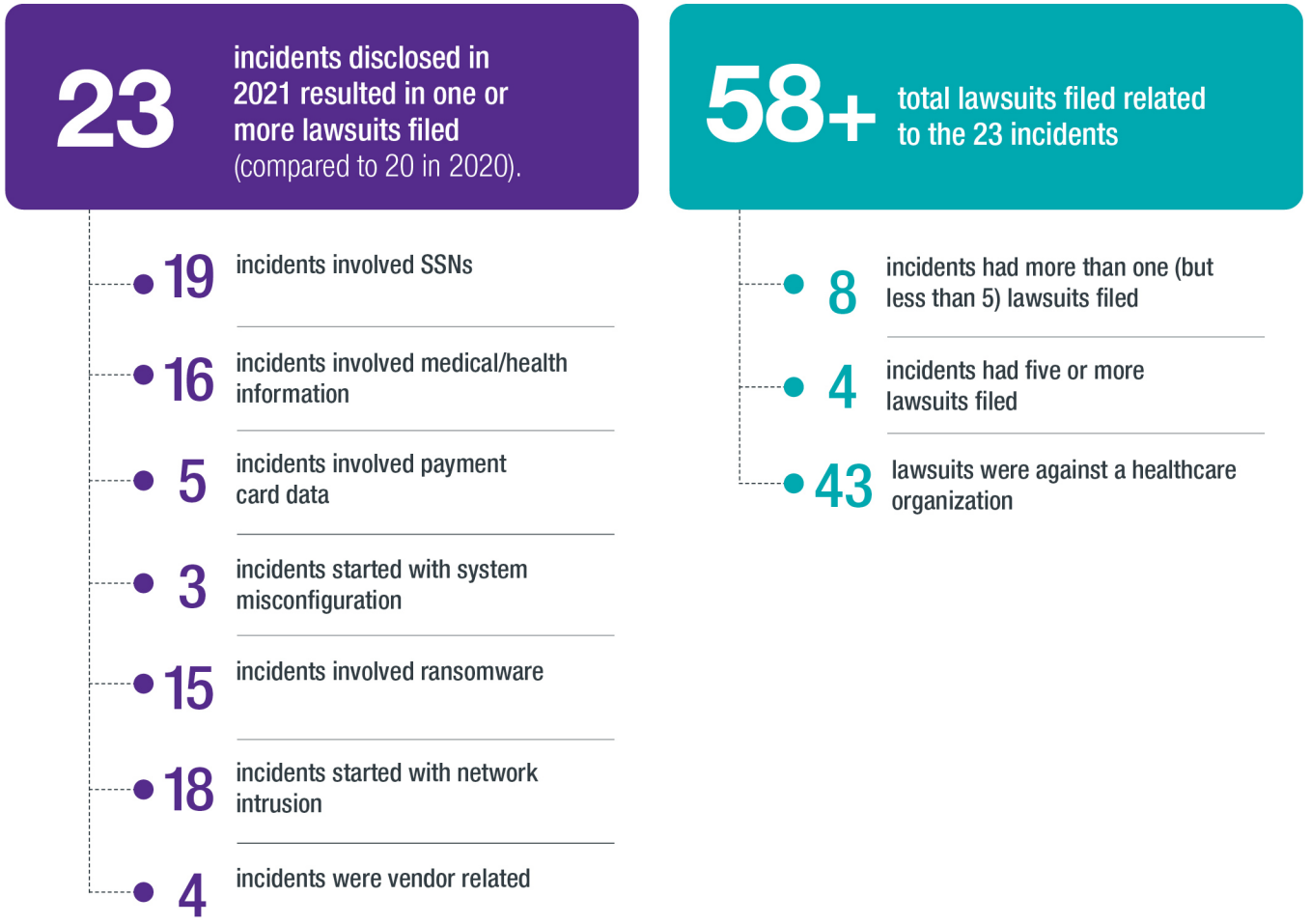
Privacy+ Security Forum

- Tort damages can include all reasonably foreseeable losses, but may be limited by the economic loss doctrine, comparative fault, mitigation and other tort concepts.
- Contract damages can include direct and indirect/consequential damages such as those necessary to meet a party's expectation, reliance or restitutionary interests, subject to contractual limitations of liability, indemnification and other provisions.
- Statutory damages can be imposed within the minimum-maximum statutory range based on a variety of factors, and may be available even absent proof of actual injury.
- The type of cyber incident can lead to a wide range of losses, including reimbursement for typical 1st party expenses, plus economic losses suffered by affected individuals and lost business, reputational harm, indemnification for fines/penalties/judgments against business customers.
  - Ransomware losses – recent anecdotal cases include losses ranging from $1 million to over $100 million in claimed damages.
  - PII/PHI data breach losses – recent anecdotal cases include losses ranging from $75,000 to $150 million, depending on the number of records impacted

Litigation Trends

Privacy+ Security Forum

- More Class Actions Are Being Filed Per Incident
- Less Cooperation with Plaintiff's Bar
- Consolidation and Transfer in Federal Court
- More Cases Litigated in State Court
- Discovery on the Horizon
- Discovery Disputes Expanding
- Privilege Battles Continue
- Certification Disputes Coming into Focus
- Trials!



SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies

FOR IMMEDIATE RELEASE
2022-39

Washington D.C., March 9, 2022 — The Securities and Exchange Commission today proposed amendments to its rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies.

FACT SHEET

Public Company Cybersecurity; Proposed Rules

1. **Form 8-K Reporting of Material Cybersecurity Incidents**. Form 8-K would be amended to add new Item 1.05, requiring issuers to disclose cybersecurity incidents within four days of making a determination that a cybersecurity incident is material.
2. **Cybersecurity Incident Disclosures in Periodic Reports**. There are two proposed changes to Regulation S-K that would require issuers to provide cybersecurity incident disclosures in their Form 10-Q or Form 10-K filings.
3. **Disclosures Related to Risk Management, Strategy and Governance**. Proposed amendments to Regulation S-K require issuers to provide disclosures related to cybersecurity policies and procedures, and governance.
4. **Disclosure Regarding the Board of Directors' Cybersecurity Expertise**. A proposed amendment to Item 407(j) of Regulation S-K would require disclosure about the cybersecurity expertise of members of the board of directors. If any member of the board has cybersecurity expertise, the issuer would have to disclose the name of any such director and describe the nature of the expertise.

FTC Act Enforcement

In re Drizly, LLC & James Cory Rellas

Privacy+ Security Forum

- Settlement related to 2020 breach involving PII for > 2.5 million users
  - Second GitHub-related incident – detected by media/social media users
  - No CISO
  - No MFA/inadequate password policy
  - No network monitoring for malicious activity
  - No/inadequate cybersecurity policies & procedures
  - Inadequate data retention/deletion practices
  - No user training
- Unanimous FTC vote to require company **and CEO** to maintain robust cybersecurity program
- Order applies to CEO for 10 years at Drizly or in any other senior exec role for co that collects > 25K consumers' data
- Order applies to Drizly for 20 years
  - Extensive program build based on under Safeguards Rule (Oct. 2021)
  - 3d party InfoSec Assessments every 2 years
  - Annual Compliance Certifications
  - Incident Reports Within 10 Days of Other Notice

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina M. Khan, Chair**
Noah Joshua Phillips
Rebecca Kelly Slaughter
Christine S. Wilson
Alvaro M. Bedoya

In the Matter of **DRIZLY, LLC, a Limited Liability Company,** **and** **JAMES CORY RELLAS, individually, and as an officer of DRIZLY, LLC.**	**DOCKET NO.**

COMPLAINT

The Federal Trade Commission ("FTC"), having reason to believe that Drizly, LLC, a limited liability company, and James Cory Rellas, individually and as an officer of Drizly, LLC (collectively "Respondents"), violated provisions of the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Drizly, LLC ("Drizly") is a Delaware limited liability company with its principal place of business at 501 Boylston Street, Boston, MA 02216. Until October 13, 2021, Drizly was a subsidiary of The Drizly Group, Inc., a holding company. On October 13, 2021, Drizly, LLC became a wholly-owned subsidiary of Uber Technologies, Inc. ("Uber").

2. Respondent James Cory Rellas ("Rellas"), is the Chief Executive Officer ("CEO") of Drizly, LLC. Individually or in concert with others, he had the authority to control, or participated in, the acts and practices alleged in this complaint.

Dispute Resolution and Remedial Measures

Privacy+ Security Forum

- Significant incidents can result in multiple, parallel investigations
- Disclosures lead to Investigations, which often overlap with Civil Litigation
- Investigations and civil litigation both focus extensively on the pre-incident cybersecurity program **and** the incident response/disclosure process
    - Did the company act reasonably in light of foreseeable risk?
    - Did the company appropriately disclose cybersecurity issues and incidents?
- Legal privilege and work product protection in the response process can have an enormous impact on litigation exposure and liability risk
- Commercial disputes may be resolved through pre-complaint ADR
- Early dismissal of civil litigation has become less likely (standing and pleading deficiencies are less likely)
- Discovery will likely be broad, long and expensive
- Pre-trial resolution is growing less likely in light of significant factual disputes

Criminal Investigations & Litigation

Privacy+ Security Forum

United States v. Sullivan

- Former Chief Security Officer/Deputy GC (and cybercrime prosecutor) convicted of obstruction of justice and misprision of a felony
- Jury convicted based on active concealment of 2016 data breach/cyber extortion incident from FTC and affected individuals
- First criminal conviction of a senior executive for obstructing a regulatory investigation into cybersecurity program compliance and concealing a cyber incident from regulators.
- Reflects whole-of-government trend in cybersecurity policy toward more robust disclosure and reporting obligations.
- Hits on the hallmarks of the DOJ's revised white collar policy prioritizing individual accountability for organizational criminal conduct.
    - Prosecution decisions will rest heavily on past history of non-compliance, current compliance programming, and whether the organization provides timely and full self-disclosure of misconduct by individuals.

PRESS RELEASE

Former Chief Security Officer Of Uber Convicted Of Federal Charges For Covering Up Data Breach Involving Millions Of Uber User Records

Wednesday, October 5, 2022

Share

For Immediate Release

U.S. Attorney's Office, Northern District of California

Federal Jury Finds Joseph Sullivan Guilty of Obstruction of the Federal Trade Commission and Misprision of a Felony

SAN FRANCISCO – A federal jury convicted Joseph Sullivan, the former Chief Security Officer of Uber Technologies, Inc. ("Uber"), of obstruction of proceedings of the Federal Trade Commission ("FTC") and misprision of felony in connection with his attempted cover-up of a 2016 hack of Uber. The announcement was made by United States Attorney Stephanie M. Hinds and FBI San Francisco Special Agent in Charge Robert K. Tripp following a four week trial before the Hon. William H. Orrick, United States District Judge.

"Technology companies in the Northern District of California collect and store vast amounts of data from users," said U.S. Attorney Hinds. "We expect those companies to protect that data and to alert customers and appropriate authorities when such data is stolen by hackers. Sullivan affirmatively worked to hide the data breach from the Federal Trade Commission and took steps to prevent the hackers from being caught. We will not tolerate concealment of important information from the public by corporate executives more interested in protecting their reputation and that of their employers than in protecting users. Where such conduct violates the federal law, it will be prosecuted."

United States v. Sullivan

Privacy+ Security Forum

- Active Concealment/Obstruction Charges
  - **18 U.S.C. § 1505 -- Obstruction of Proceedings before a Department or Agency of the United States**
    - Whoever corruptly . . .influences, obstructs, or impedes or endeavors to influence, obstruct or impede the due and proper administration of the law under which any pending proceeding is being had before any department or agency of the United States . . . shall be fined . . . imprisoned . . . .
  - **18 U.S.C. § 4 – Misprision of a felony**
    - Whoever, having knowledge of the actual commission of a felony . . . Conceals and does not as soon as possible make known the same to some judge or other person in civil or military authority under the United States shall be fined under this title or imprisoned not more than three years, or both

United States v. Sullivan

Some Initial Takeaways

Privacy+ Security Forum

- Avoid active concealment of information about security incidents and extortion payments.
- Ensure that bug bounty programs have proper parameters that are followed.
- Be prepared to be investigated – and not just by regulators
  - Other IR team members, executives – and even the hackers – may be witnesses against you.
- Brace for intense discovery/privilege battles with criminal defendants (and the government)
- Expect increased whistleblower activity related to cybersecurity programs and incidents

Questions & Contacts

Privacy+ Security Forum

Ed McAndrew
Partner, Cybersecurity & Litigation
BakerHostetler
202-664-2939
emcandrew@bakerlaw.com

Nate Lovett
Associate
Insurance & Privacy, Cyber & Data Governance
Wiley Rein LLP
202-719-7295
nlovett@wiley.law

James Perry
Senior Director of Consulting Services
CrowdStrike