

Open SSL Conference

# From Bug to Breach: Legal Lessons in Cryptographic Failures

Presented by Ashley Pusey, CIPP/E/US, CIP,  
FIP

October 2025

## **DISCLAIMER**

This presentation and its contents are provided 'AS IS', without warranties or conditions of any kind.

- No guarantee as to accuracy, completeness, or applicability
- Nothing herein constitutes legal advice
- All examples are illustrative only
- By relying on this material, you assume all risks

# Setting the Stage

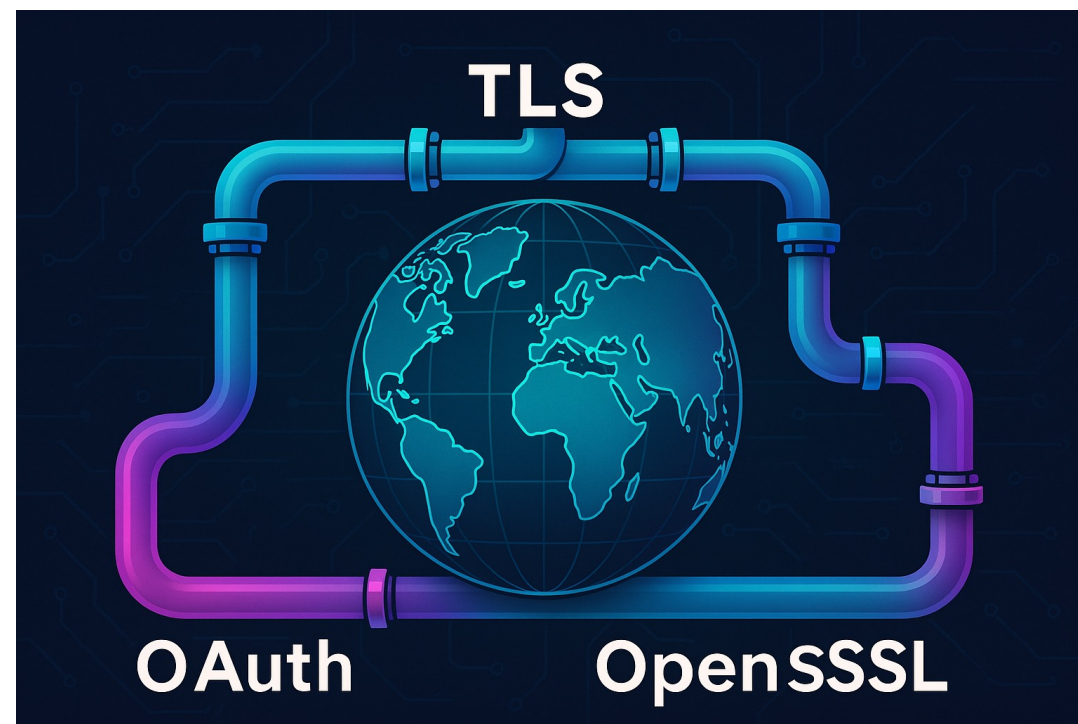
## Every System Has Pipes

- Data systems can be viewed as your organization's plumbing infrastructure
  - Valves = authentication controls
  - Pressure gauges = logging & monitoring
  - Pipe joints = integrations
- Leaks happen because a fitting fails
- Leaks = incidents
- Incident = potentially open up legal flood gate

# The Internet Runs on Open Source

## Shared Code Doesn't Necessarily Mean Shared Liability

- Plumbing runs behind the walls → open source runs beneath the apps
- Most companies don't install their own pipes – but they rely on them daily
- Small leak in your infrastructure can become a flood in liability or result in regulatory inquiries (or both)



# The Duct Tape – DIY Temptation

## Fast or Temporary Fixes = Disasters

- A temporary dev shortcut can open an organization to legal exposure
- Relying on legacy encryption and outdated security controls
- Leaving “temporary” configurations (expired certificates, deprecated protocols)
  - Equifax (2017): PKI certificate expired for 10 months → security tools couldn’t inspect encrypted traffic → attackers hid for 76 days.
- Every outdated control that remains in place quietly expands legal exposure
- Don’t let the duct tape be your infrastructure

# 1<sup>st</sup> Response Protocols

## Who's Your First Call

Step	Role	Why First
1. Outside Counsel	Directs investigation; establishes privilege	Ensures findings & comms protected
2. Cyber Insurance Carrier	Activates breach coach / vendors	Preserves coverage, avoids late-notice denial
3. IT / Forensics (via counsel)	Executes containment	Keeps technical work under privilege

# Legal & Regulatory Frameworks Potentially Triggered

Framework	Trigger	Time to Notify	Who's Notified
HIPAA / HITECH	PHI breach or unauthorized access	60 days	OCR + affected individuals
GLBA / FTC Safeguards	Unauthorized acquisition 500+ person	Without unreasonable delay, No later than 30 days	FTC
State Breach Laws (50+)	PII of residents	30-60 days	State AGs + consumers
CCPA / CPRA (CA)	Personal data exfiltration	"Without unreasonable delay"	CPPA Board + Californians
SEC Cyber Disclosure	Material cyber event	4 business days post-materiality	SEC (Form 8-K)
GDPR / UK DPA	EU/UK resident data	72 hours	Supervisory authorities
Insurance Policy Conditions	"Security Incident" or "Claim"	As specified in policy	Carrier

# When the Inspector Knocks

Regulators are the building inspectors of your digital plumbing. They don't just check for leaks — they audit your blueprints.

- Regulators = Plumbing Inspectors of the Digital Age (GDPR, FTC, SEC, HIPAA)
- Once a breach is reported, the inspection begins — regulators (OCR, FTC, SEC, state AGs) look backward, not just at the incident
  - Ex: Under HIPAA, OCR routinely issues data requests asking for 6 years of security policies, invoices, risk assessments, and control documentation.
- If security and data protection controls are not in place, make it more difficult to make a case to the regulator
  - Security controls weren't documented or the organization did only the bare minimum.
- If it's not documented, it didn't happen.



# Scenario

## Is there a leak or did the pipe burst?

You're corporate counsel at DataForge, an AI-enhanced customer relationship platform, with an integrated chatbot add-on called ChatFlow, (build by Saleslyft).

On Tuesday morning, your CISO Slacks you:

*We've detected unusual access patterns through an integration partner, but we don't have any signs that our system was directly breached. ChatFlow says it's investigating.*

# Scenario

## Investigation Remains Ongoing

An internal investigation confirms that DataForge's systems were not compromised.

*Meanwhile ....*

Attackers compromise SalesLyft's GitHub (the vendor that powers ChatFlow), adding a guest user and downloading integration repositories.

Attackers move laterally into SalesLyfts's cloud, extracting OAuth tokens used to connect customer ChatFlow instances with DataForge.

- They didn't break the pipe, but they stole the master valve keys.
- Tokens grant access to **DataForge CRM** APIs → attackers run bulk queries, exporting case data.
- Valid tokens — still unauthorized?

# Scenario

## TA Claims

TA Claims they stole data from chat bot, and other customer data, including 500 million records of contact information.

Proof of acquisition exchange occurs.

You confirm that the items on the file tree.

# Scenario – Phase 2

## The Ransom Note

*Ransom:*

*“This message serves as formal notification that DataForge has been hacked by us and faced a major information security breach. Contact us to negotiate this ransom, or all your customers’ data will be leaked. Failure to meet these demands will ultimately have us release all of the compromised data, and you will be dealing with the escalation of all consequences described above. Because you had no preventive measures in place, you will be dealing with them a lot.”*

You learn that the threat actors have information of major global companies, and the hackers are threatening to release around 1 billion records with personally identifiable information.

The TA further accuses that your company did not have two-factor authentication (2FA) or any other type of OAuth security.

# Scenario – Phase 2

## Investigation Remains Ongoing

### *Initial Triage*

- Unauthorized access to regulated data
- Compromised crypto tokens
- Extortion = confirmed disclosure
- Late or incomplete notification
- Vendor oversight failure
- Misalignment of technical vs legal definitions

\* 4- 6 weeks pass for the forensics investigation.

### *Forensics Confirms*

Between September 8 and 18, stolen tokens are used to query DataForge CRM data (Cases, Contacts, Credentials).

TA subsequently posts data online.

# Audience Poll: When Did the Breach Occur?

- A. GitHub compromise
- B. Token theft
- C. Data access / proof of exfiltration exercise
- D. Extortion post
- E. Data publication

# Let's connect!



**Ashley Pusey**

Associate  
New York


+1.646.625.3998


[ashley.pusey@kennedyslaw.com](mailto:ashley.pusey@kennedyslaw.com)

**Ashley Pusey, CIPP/US/EU, CIPM, FIP**  
Privacy, AI & Cyber Attorney  
| Translating Complex Tech & Pri...




# Kennedys

 Kennedys

 KennedysLaw

 KennedysLaw

 KennedysLaw

Kennedys is a global law firm operating as a group of entities owned, controlled or operated by way of joint venture with Kennedys Law LLP.  
For more information about Kennedys' global legal business please see [kennedyslaw.com/regulatory](https://kennedyslaw.com/regulatory)

[kennedyslaw.com](https://kennedyslaw.com)