Breach Response Considerations for the Convenience Store and Petroleum Market

Presenter:

Todd McClelland

Partner, McDermott Will & Emery LLP

CONEXXUS
solve forward

Agenda

- Housekeeping
- Presenters
- About Conexxus
- Presentation
- Q & A

Presenters

Conexxus Host

Allie Russell
Standards Coordinator
Conexxus
arussell@conexxus.org

Moderator

Kara Gunderson
Chair, Data Security Committee
POS Manager, CITGO Petroleum
kgunder@citgo.com

Speaker

Todd McClelland
Partner, McDermott Will & Emery LLP
tmcclelland@mwe.com
(404) 483-6976

CONEXXUS
solve forward

About Conexxus

- We are an independent, non-profit, member driven technology organization
- We set standards…
  - Data exchange
  - Security
  - Mobile commerce
- We provide vision
  - Identify emerging tech/trends
- We advocate for our industry
  - Technology is policy

2020 Conexxus Webinar Schedule

Month/Date	Webinar Title	Speaker	Company
January 23, 2020	How to elevate your business through digital transformation	Dean Marier	Cybera
February 27, 2020	Progress in the “API Sprint”	Gray Taylor David Ezell	Conexxus Conexxus
March 18, 2020	Data Security Beyond PCI: Securing the Enterprise	Ed Adams Marc Punzirudu Kara Gunderson Sam Pfanstiel	Security Innovation ControlScan CITGO Petroleum ControlScan
April 2, 2020	Presentation by GS1	Liz Sertl	GS1
May 7, 2020	Breach response considerations for the convenience store and petroleum market	Todd McClelland	McDermott Will & Emery
June 2020	How an attacker bypasses network, software and physical controls	Geoffrey Vaughan Jeff Gibson	Security Innovation ControlScan
July 2020	PCI DSS 4.0	Troy Leach	PCI SSC

CONEXXUS
solve forward

2020 Conexxus Webinar Schedule

Month/Date	Webinar Title	Speaker	Company
July 2020	POS Managed Network Service Program		Joint MNSP's
August 2020	Vulnerability & Patch Management – Retail Operations		POS Vendors
September 2020	TBD	Scott Cheek	SageNet
October 2020	Ransomware Protection and how a Managed Security Service Provider can help Oil & Gas Retailers from being the next target	Ajith Edakandi	Hughes Network
November 2020	TBD	Ash Swamy	Omega
December 2020	Enterprise data security best practices - Cybera API webinar with David - Stuzo		

CONEXXUS
solve forward

Thank you to our 2020 Diamond Sponsors

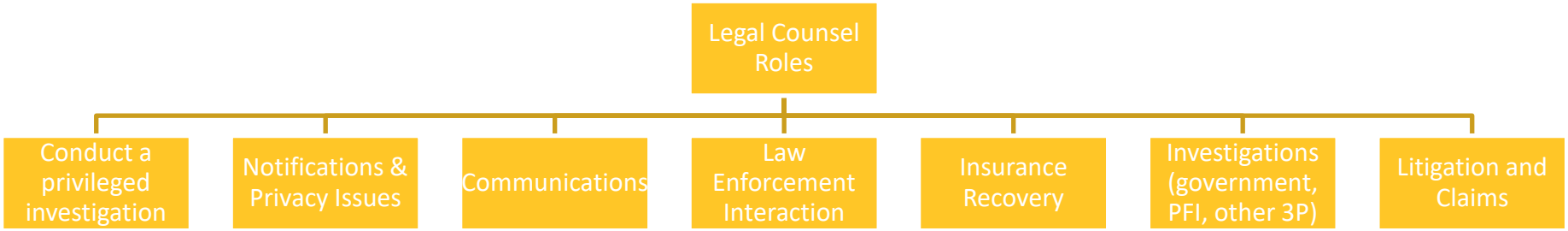
How Incidents are Discovered

CONEXXUS solve forward

Initial Response is Key

- Engage counsel
- Review your Incident Response Plan
- Consider internal escalation (who needs to know)
- Identify “the team” (excluding those who don’t need to know)
- Internal v. external forensics
- Consider insurance notice
- Consider evidence preservation (logs, server images, workstations, mobile devices)
- Identify initial notification requirements
- Is it public?

Working with legal counsel



The Attorney-Client Privilege & Work Product Doctrine

A/C Privilege:

Protects confidentiality of communications between lawyers and clients

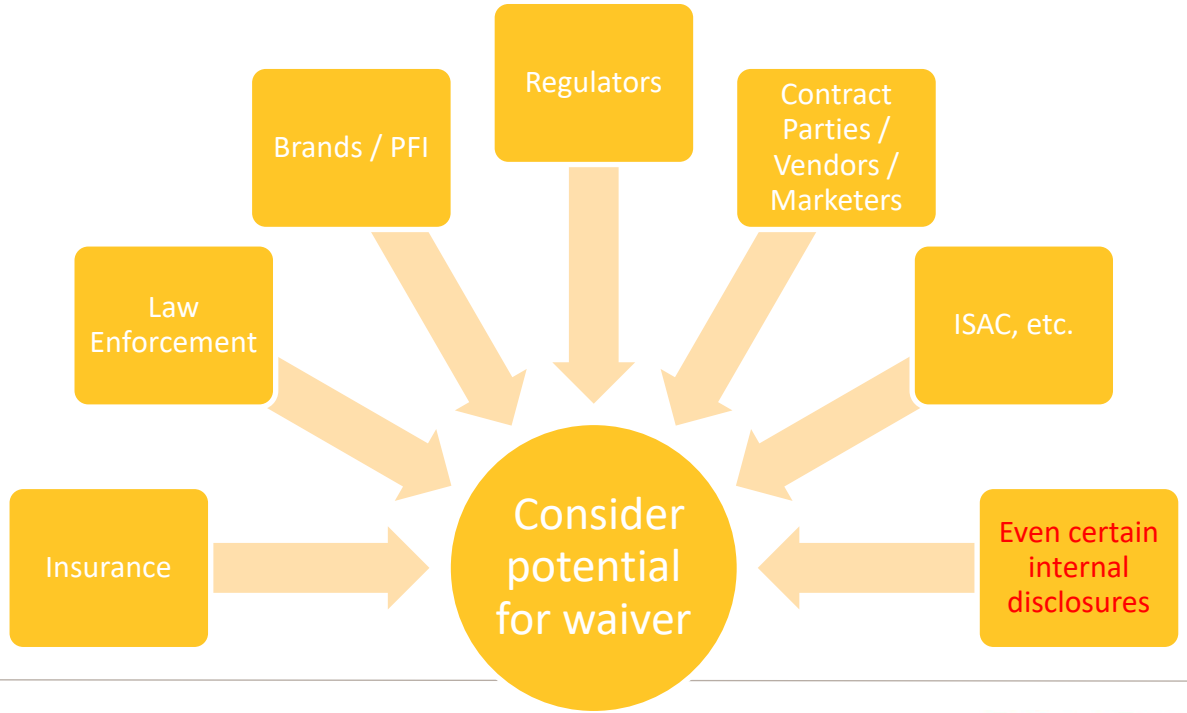
Issue:
What we can protect
v.
what we want to protect

Work Product Doctrine:

Protects certain documents and materials prepared in anticipation of litigation

CONEXXUS
solve forward

Waiver?
Be careful with disclosures to:



CONEXXUS solve forward

Protection Limitations with Forensic Investigations

- Doesn’t protect facts!
- Doesn’t apply to business functions
- Documents prepared for another purpose are at risk.
- Can’t just copy counsel
- Counsel must actually lead the investigation
- Forensics should be engaged by counsel
- Limit disclosure of findings, conclusions and protected communications

Notification

- Direct to payment brands
- Legal notice to consumers and regulators
- Contractual (processor/acquirer)
- Contractual (franchisees)
- Contractual (vendors and service providers)
- Law enforcement

PCI Notification Requirements

- These change. Check most recent requirements!
- Your processor/acquirer contract likely has requirements
- Visa, Mastercard, Amex, Discover – varying triggers:
  - Unauthorized access to cardholder data
  - Unauthorized access to the payment system
  - Unauthorized manipulation of account data controls
  - Unauthorized access to encryption keys

Visa

Visa, October 2019, What To Do If Compromised:

“An entity that suspects or confirms unauthorized access to any Visa payment account data, or to any payment system that stores, processes or transmits Visa payment account data, is required to ensure that the Compromise Event is reported to the Visa Risk Management group within three (3) calendar days of either (a) the discovery of evidence sufficient to raise a reasonable suspicion of a Compromise Event, or (b) the discovery of evidence sufficient to confirm the existence of a Compromise Event beyond a reasonable doubt.”

Visa

Visa, October 2019, What To Do If Compromised:

Within three (3) calendar days of notifying Visa pursuant to Section 1.1., above, provide a report describing the event (the Incident Report) to Visa and the Acquiring bank (if applicable). Please refer to Attachment A at the end of the document for an editable copy of the Incident Report.

Mastercard

Mastercard February 14, 2019, Security Rules and Procedures:

Within twenty-four (24) hours, and on an ongoing basis thereafter, submit to Mastercard all known or suspected facts concerning the ADC Event or Potential ADC Event, including, by way of example and not limitation, known or suspected facts as to the cause and source of the ADC Event or Potential ADC Event to the satisfaction of Mastercard.

PCI Forensic Investigators (PFI)

- Time to engage a PFI
  - Visa = at its discretion; must contract within 5 business days
  - Mastercard = required; must engage within 72 hours
- Suggestion: Retain now
- Not a privileged investigation!
- The PFI Report

Franchisees, Wholesalers, Marketers, etc.

- Who is the Merchant of Record?
- Review your contracts
- Notification obligations?
- Indemnity?
- Brand Impact

Vendors and Service Providers

- Vendor/Customer interests often diverge during a breach.
- Know your contract:
  - Notice timing
  - Liability
  - Audit rights
  - Information sharing
  - Notification obligations
- Some laws impose notification obligations directly on vendors
  - This possibility could change your notification analysis!

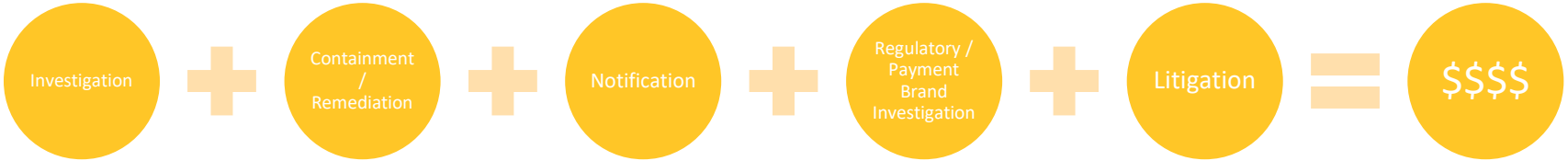
Brand Impact

- Communications are key -- control the narrative
- Consider a PR firm
- Review social media, blogs, information sharing and knowledge centers (ISACs), Krebs, etc.
- Anticipate that employees will talk
- Limit third party disclosures
- Communications must be consistent!

What happens after a breach

- PFI and the Brands
- Regulator investigations
- Civil litigation
  - Consumer class actions
  - Issuer claims
  - Shareholder derivative suits
  - Contract claims

Cost of a Breach

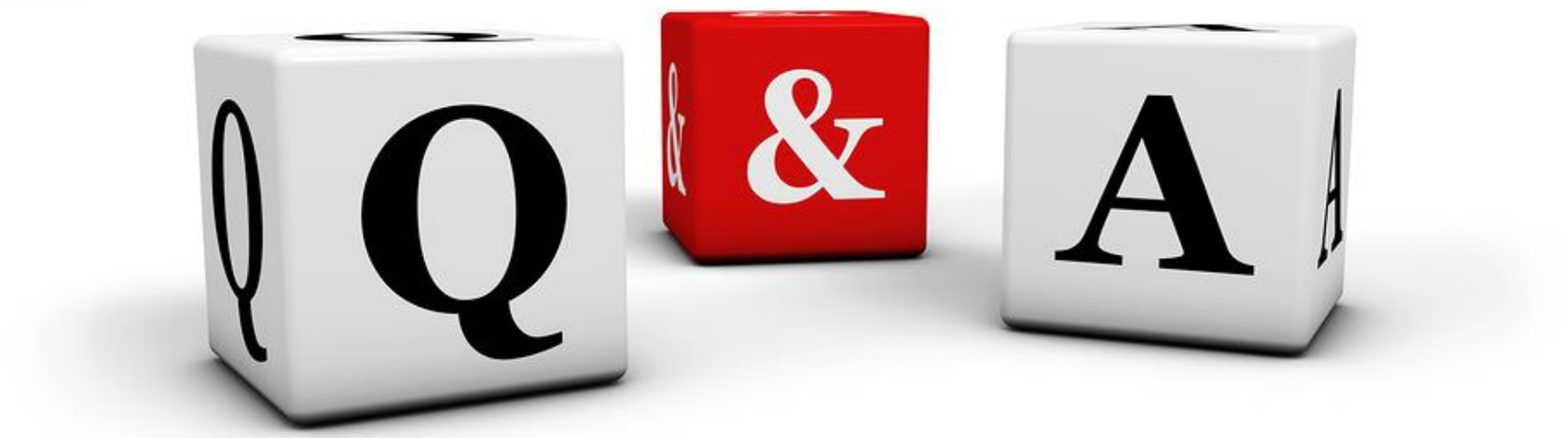


What they don’t tell you

- Breach fatigue sets in early
- Information will leak – plan on it
- Frequent and tricky question - Is it contained?
- When to end the investigation?
- Documentation, emails, and reports
- Working with law enforcement
- Confirming vulnerability remediation

Breach Prep Checklist

- Engage a PFI
- Engage external counsel
- Engage external forensics (through counsel)
- Review your IRP
- Do regular tabletop & training – specifically prep for a franchisee incident
- Know your CSIRT (who leads?)
- Check logging and retention
- Check key vendor contracts
- Review your cyber liability insurance – have a cyber insurance attorney review as well.
- Identify notification requirements
- Check law enforcement contacts
- Data governance: Map your data
- Maintain your CMDB
- Engage in future vendor contracts, expecting a breach



CONEXXUS
solve forward

- Website: www.conexxus.org
- Email: info@conexxus.org
- LinkedIn Profile: Conexxus.org
- Follow us on Twitter: @Conexxusonline

DISCLAIMER: Conexxus does not endorse any products or services that may be described or mentioned in this presentation. The views and opinions expressed in this presentation are solely those of the speakers and not of Conexxus. By hosting this webinar, Conexxus is not providing any legal advice; if you have any questions about legal issues raised or discussed, you should seek the assistance of attorneys who are competent in that area.