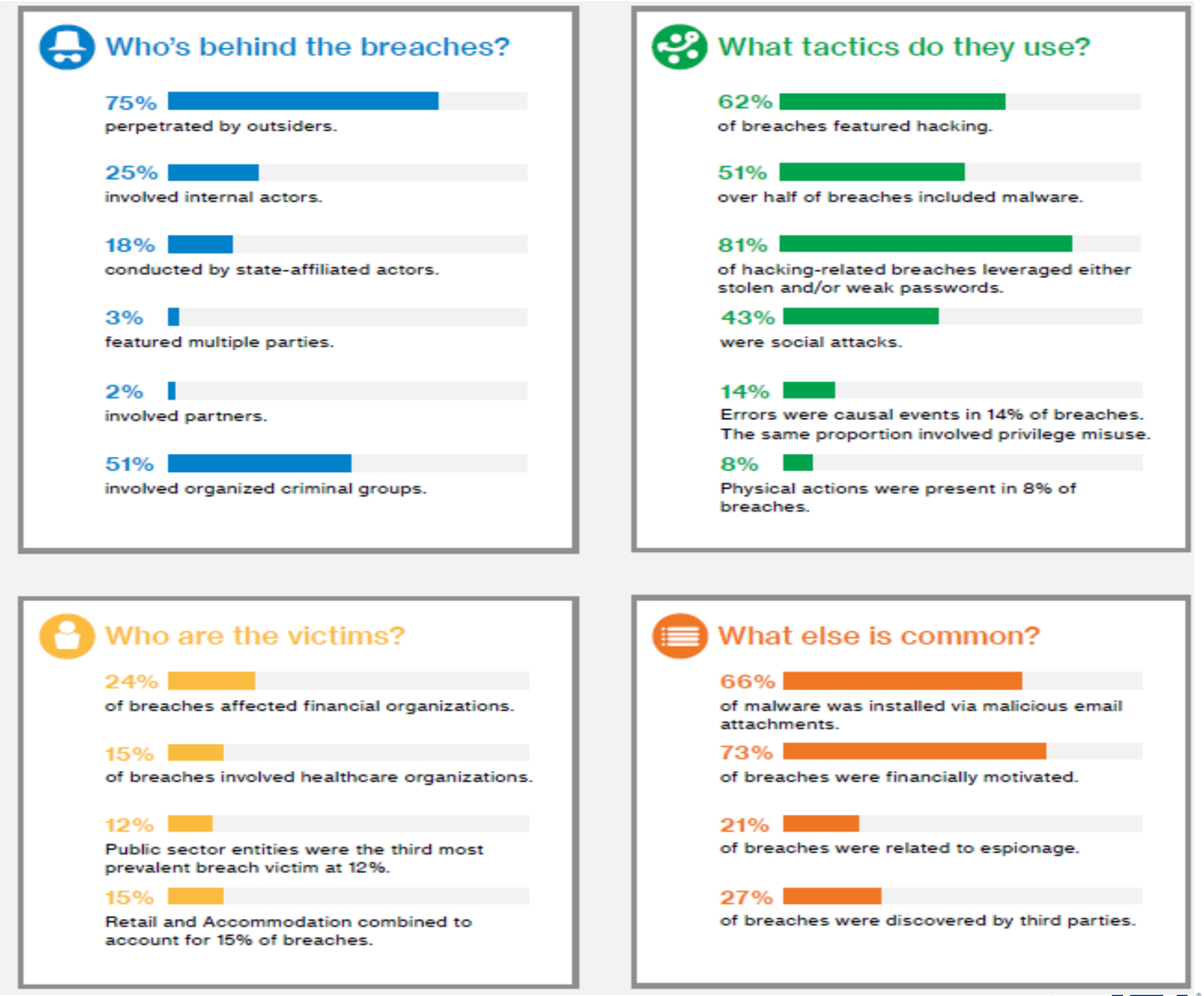

2018 IFA
LEGAL
SYMPOSIUM
May 6-8 | Washington, DC
IFA
INTERNATIONAL FRANCHISE ASSOCIATION

Data Security and Addressing the Risks in the Franchise System

- JoAnn Carlton
- Heather Enlow-Novitsky
- Matthew Fore

By the Numbers

Source: 2017 Verizon Data Breach Investigations Reports



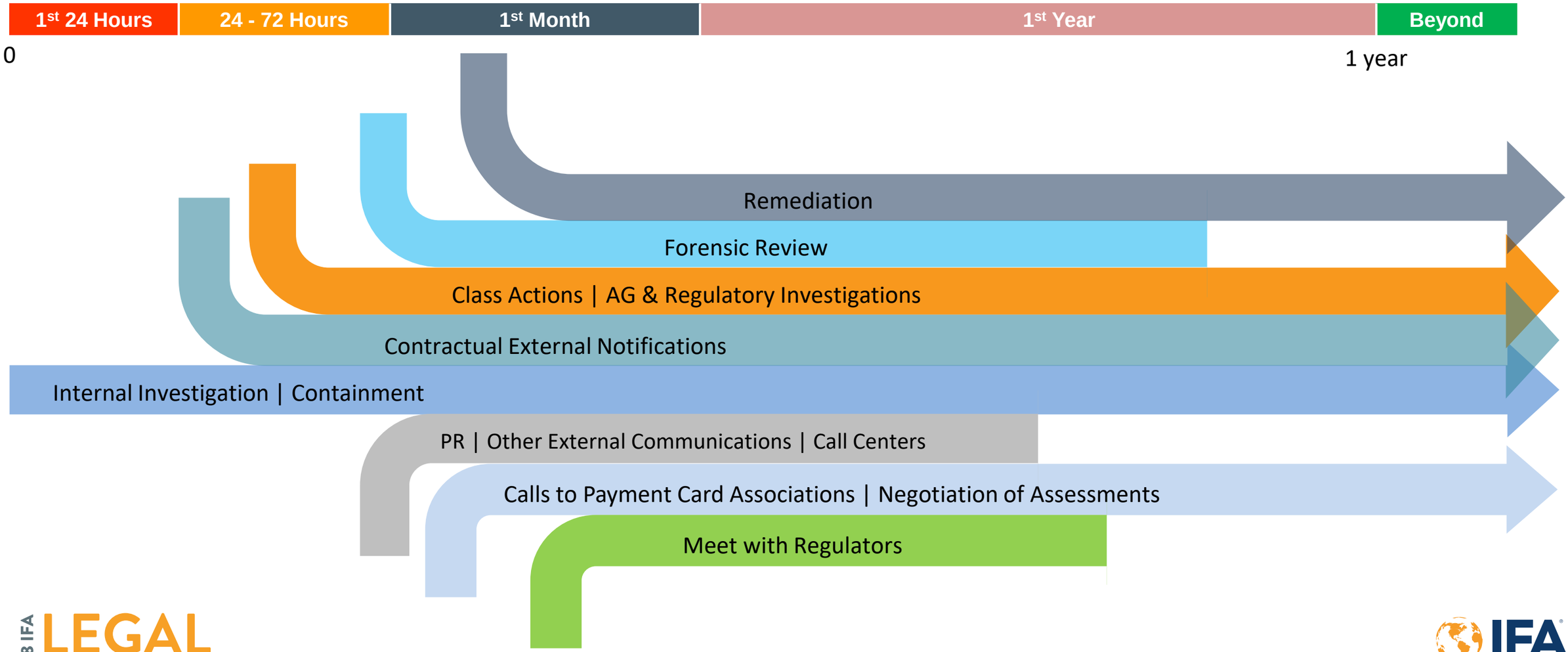
When an incident Occurs Multiple Demands Ensue

- Customers
- Employees/Franchisees
- Containment
- Remediation
- Forensic Investigators
- News Media/Bloggers
- Vendors
- Payment Card Brands
- Regulators
- Lawsuits

What to do When You Have an Incident?

- Follow your Incident Response Plan
  - **Internal steps**: Containment/Remediation
    - Determine how the breach occurred
    - Set up safeguards to prevent reoccurrence
    - Document the breach, steps taken to prevent and how to improve
  - **External steps**: Notification
    - Law enforcement
    - Card Brands
    - Customers
    - Franchisees/Employees
    - Regulators
    - Business partners
    - Insurers

Coordinating Response



Phase One – The First 24 Hours

- Alert the Core Team
  - Determine the nature and scope of the incident
    - What type(s) of data are at risk
    - When did the compromise begin
    - What is the potential scope
  - Assess priorities and risks
  - Is the incident contained?

Phase Two – The First 24-72 Hours

- Contact law enforcement
- Activate independent/privileged forensic investigator
- Make initial notifications to Payment Card Associations, payments processor and acquiring bank
- Select and activate PFI Investigator
- Review notice obligation to insurer(s)
- Satisfy other contractual notice obligations

Attorney-Client Privilege

- Protects communications pertaining to legal advice
- Communications are privileged – underlying facts are not
- Must be made in confidence
- Can be waived

Work Product Doctrine

- Protects attorneys':
  - Thoughts
  - Mental impressions
  - Conclusions
  - Opinions or legal theories
- Must be made in anticipation of litigation
- Materials prepared in ordinary course are not protected
- Facts may be discoverable if there is substantial need and an inability to obtain it through other means

Tips for Privileged Investigations

1) Establish that legal advice or services are sought by the company
2) Involve outside counsel
3) At the direction of counsel
4) Privileged forensic experts engaged to assist counsel
5) Litigation hold

Tips for Privileged Investigations (cont'd)

6) "Need to Know" basis

7) Conduct appropriate employee interviews

8) Communications with former employees limited to what employee knew when employed

9) Mark privileged documents as such

10) Consider a "Common Interest Agreement" with affected third parties

Phase Three – The First Month

- **Starts with Internal Communications**
  - Information for employees and franchisees
  - Scripting for calls to Call Center & Help Line
- **Then, External Communications**
  - Statutory notifications
  - Press releases, FAQs across all media
  - Social Media response
  - Business Partners
  - Risk Management – Insurance
  - Calls with Payment Card Associations
- **Customer Communications**
  - Protect the Customer and make them whole; protecting the customer protects the brand.
  - Ensure communications are accurate and timely. Balance timely against avoiding premature notice.
- **Who will be the face of the company?**

Phase Three – The First Month (cont'd)

- **Investigations/Lawsuits/Remediation**
  - Remediation plans must be started
  - Card brand contractual liability and assessments
  - FTC Investigations
    - Was there "reasonable" security? Document it now.
    - What was the business purpose for collecting or retaining the data?
  - State AG Investigations
  - Lawsuits
    - Employees
    - Customers
    - Issuing Banks
    - Shareholders

Phase Four – First Year and Beyond: More to Come

- Review and finalize the forensic report (3-9 months)
  - Independent Forensic Investigator can be integral
- PFI Reports
  - Remediation plan is to be submitted within 5 business days of the final Forensic Report
- Demonstrate compliance with data security standards
- Ongoing negotiations of assessments with Payment Card Associations (1-2 years)
- Responding to inquiries from regulatory investigations; meetings and negotiations (1-3 years)
- Resolving litigation

Preparing for Your Response

- Prepare a written Incident Response Plan
  - Select and train your team
  - Refine workflow process – emphasis on coordination and escalation
  - Inventory contractual notice obligations
  - “Interview” incident response vendors
  - Identify law enforcement contacts
- Practice
  - Conduct “Tabletop” exercises

Card Brand Update

- Each Card Brand is different
  - Notification requirement 24-48 hours
  - Fines for violations of PCI-DSS
  - Card replacement and monitoring
  - Counterfeit fraud (card present)
  - Case management fee eliminated by all brands now

Franchise System Issues

- Assisting with franchisee investigations/concerns
- Control of the payment system/applications
- Mandated vendors and other measures
- Liability concerns – how divided?

Lessons Learned from Other's Mistakes

- Escalate a reported incident quickly and efficiently
- Ensure that entire response team has an understanding of the attorney client privilege and work product doctrine
- Do not make overstatements or unsupported promises
- Test your webpages thoroughly
- Do not register domains too far in advance of public notification
- Do not hire hackers to cover up your breach

- This is an exercise designed to help you think about and discuss what should be included in your company's response plan.
  - It is not a test of your company's technical response or whether the scenario could actually occur.
- This is practice, respond to the scenario as if this were a real event.
  - There are no wrong answers
- Everyone participates.

February 1

- Your IT team informs you that they have received a call from one of your larger franchisees requesting assistance.
- The franchisee's has been contacted by a hacker claiming to have all of its data, including customer data, payment card data, and employee SSN's.
- The hacker has requested $100,000 in Bitcoin within 5 days
- The franchisee's entire network is down and they are unable to access their systems.

February 2 – 8 am

- The franchisee's stores remain closed.
- The franchisee provides their own HR, payroll, and database systems, but you mandate use of certain point of sale equipment, and payment application software in the storefront, e-commerce and mobile channels
- The franchisee is unable to pinpoint which systems are affected, and insists it must be an issue at corporate.

February 2 – 5 PM

- Information security is able to determine that corporate systems are not affected
- Point of sale and payment application vendors have confirmed no issue.
- Franchisee is able to get their store point of sale equipment running and open stores.

February 5 – 9:30 AM

- Franchisee is approaching the deadline and insisting on advice/help from corporate.

- What does your company do?

March 17

- Friday, as your head of internal security is leaving for the weekend, he receives a call from a Secret Service agent in the local field office.
- The agent states they are seeing posts on the Dark web offering for sale credit and debit card numbers, customer names and addresses and employee SSNs claiming to be obtained from your company.

March 20

- The IT team investigates over weekend, doesn't find any signs of suspicious activity.
- However, that morning your card processor contacts you and states both VISA and MasterCard have issued CPPs. The CPPs include both franchise and corporate locations.
- Card brands are requesting a PFI be engaged.

March 28

- The PFI discovers that three IP addresses belonging to known threat actors were connecting to your payment processing gateway used by both corporate locations and franchise locations.
- The investigation reveals security flaws within the gateway due to a recent upgrade released in the fall and testing failed to catch it.

March 29

- Administrative credentials were also found on the payment application webserver with a suspicious initialization file.
- At the same time, a reporter from the Wall Street Journal contacts your company requests a statement regarding reports that issuing banks have identified you as a CPP.

April 7

- Multiple employees and notify the General Counsel that fraudulent tax returns have been filed in their names, and inquire whether this is related to the recently announced payment card breach.
- The PFI investigation reveals that the unauthorized access to the payment application also exposed other sensitive information housed in your company's systems.

Ongoing

- The investigation determines that over 5 million unique current and former customer, employee and franchisee records were potentially accessed by the known threat actors.
- General Counsel receives letters from the FTC and State Attorneys General requesting additional information.
- Multiple class actions are filed against you on behalf of the customers, and employees whose data was stolen.
- VISA notifies your processor that the event will qualify for GCAR; the processor expects a similar determination from MasterCard.
- Several issuing banks file a class action alleging fraud on the cards they issued was caused by your breach.
- Franchisees demanding corporate cover their costs since breach occurred at mandated gateway.

Questions?