ZwillGen PLLC

Critical Updates for Mitigating Privacy, Data and Cyber Security Risks in the Emerging Payments Market: Endeavoring to Use New Technology and New Business Practices to Plug the Holes

Amy Mushahwar &
Mercedes Tunstall

2014/5 –Retail Carding Breach Bonanza

- Home Depot
- UPS
- Michaels
- P.F. Chang's
- Goodwill
- Jimmy John's
- Dairy Queen

To name a few…

Payment Card Data Breaches
CNP Attacks are in the Cross Hairs

- Given that brick and mortar retailers are adopting better security practices (such as, immediate encryption at the swipe terminal, direct-to-processor communications and EMV secure chip technologies), **e-commerce and other card not present (CNP) payment card attacks are prevalent and will become more so.**
- When payment card data is at issue, there are additional notice obligations such as to:
  - Merchant Acquiring Banks / Processors (by contract)
  - Payment Card Brand (Account Data Compromise Rules, MasterCard's rules are most developed)
- Notice is typically "immediately" which is within 24 hours of a discovery of a compromise or suspected compromise of card data.

Emerging Payments – New Technology = New Vectors for Hack

- Importance of Designing Products with Security in Mind
- Consider Authentication to Existing Platforms (i.e., Apple Pay)
- Don’t run to market without fulsome security audits (PCI, ISO, COBIT, NIST, etc.)
- Understand your data flows on an end-to-end basis – don’t point fingers to a vendor

Information Sharing?

- FDIC Guidance to Participate in FS-ISAC
- Information sharing alone is not the end all and be all – knowledge must be operationalized in a SIEM, IDS/IPS, etc.
- Understand the level and posture of advice being provided
- Sharing alone won't significantly reduce the likelihood of a breach… it will help with threat detection

Detection… Automated Tools Are Great, But….

- Your IT departments are likely inundated with alerting (IDS/IPS, Antivirus, Antimalware, SIEM, Device Monitoring)
- If they have alerts your company cannot answer… smells like negligence
- There are tools to help sort through the white noise of the multiple and conflicting reports
- Tools still require careful staffing

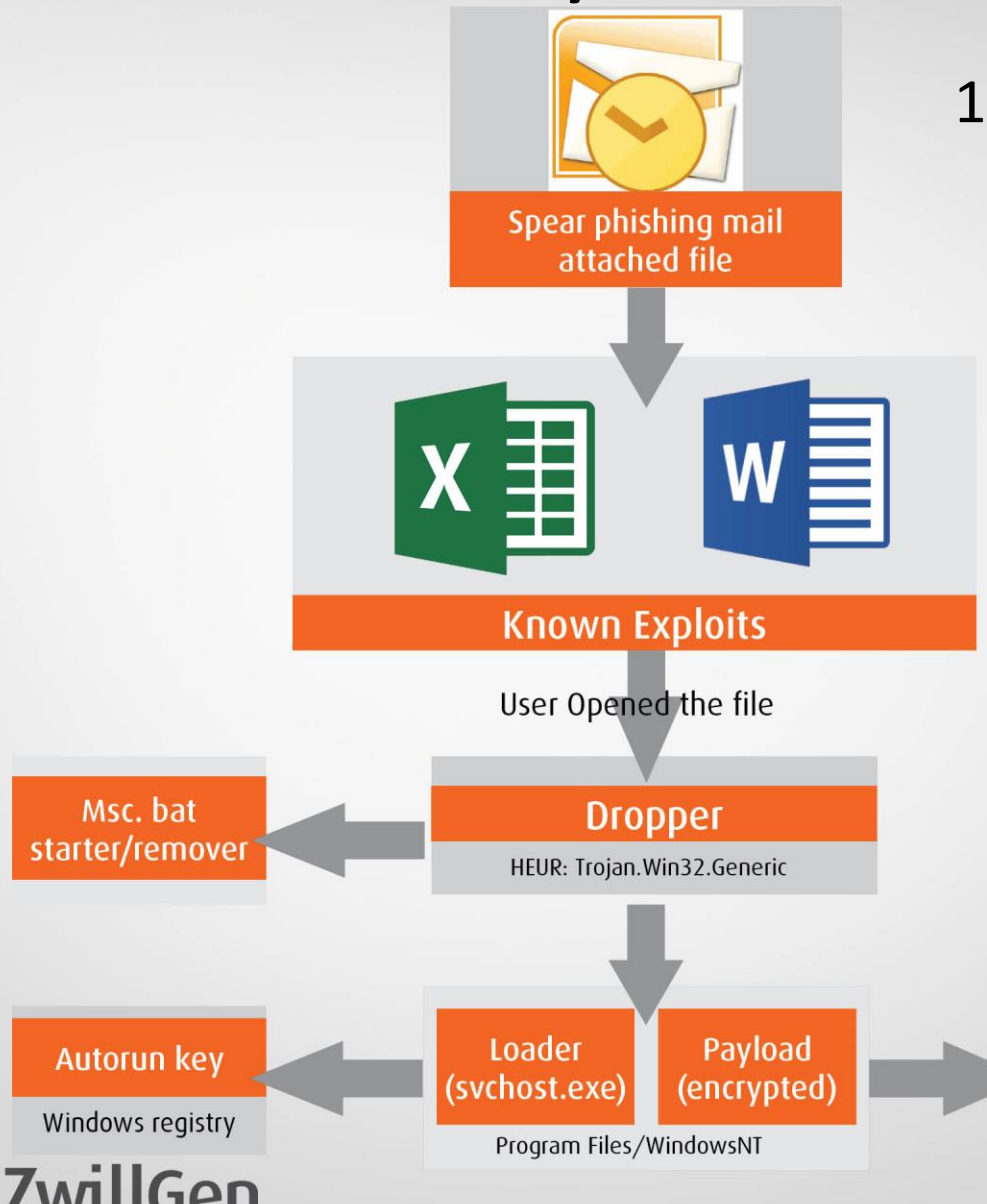
ZwillGen PLLC

Data Breaches: Why do they occur?

What is the Threat Landscape

- Criminal groups – domestically and internationally
  - Obtain credentials necessary to gain access to users other accounts or resources. Email accounts can be used for impersonation and to commit identify theft (the password may also work on the customer's other personal or corporate accounts).
  - Hackers can gain access to email accounts to send spam, spread malware and support phishing scams.
- Hacktivists
  - Target high-profile individuals and companies to embarrass them or to make a political statement about their conduct or investment decisions.
  - Accounts can be filled with scandalous information, gossip, nude pictures
- Foreign Governments
  - State-sponsored hacking is widespread and prevalent – for investment information, trade secrets and to build capability
  - U.S. government has recently found dormant Russian malware embedded in systems. If it's there…

Anatomy of a Attack



1st Stage of Attack

Not so funny point: we had a client that kept getting re-infected with malware because an employee used a POS register to charge his phone. POS machines a 'clean machines' for a reason.

Methods of Attack

- Password theft (e.g., brute force attack).
- Network hacking (e.g., exploit vulnerable code).
- Hijacking websites (e.g., create false links to real websites).
- Security vulnerabilities on mobile devices.
- Watering-Hole Attacks (putting malware on blog sites)
- Social Engineering
    - Phishing (stealing credentials or planting malware).
    - Pretexting (fooling person or business into giving up information for what seems to be a legitimate purpose).
    - Impersonation threats (e.g., email hijacking, allowing hacker to send emails that look like they are from someone you know).

Data Breaches: Why do they Occur?

Personal / Syndicate Financial Gain from Mass Data Theft

From underground websites criminals can: order a hit, rent compromised computers to attack, advertise the ability to steal data and ultimately sell data. We have seen the following rates* for consumer data:

Mother's Maiden Name	$3.00
SSN	$3.00
Date of Birth	$0.50
Mother's Birthdate	$1.00
Driver's License No.	$8.00
Credit Cards	$5.00 - $40.00 (varies on card type / age)
Criminal Background Reports	$15.00
Credit Reports	$25.00

**List not exhaustive and rates constantly vary.*

ZwillGen PLLC

Lawyers' Roles in Reducing Likelihood or Consequences of a Breach

What can Lawyers do?

- Understand Regulator and PCI Council expectations
- Understand contractual commitments
- Advise product/business people of the risks and consequences of poor security
- Understand what security measures the business has in place (SIEM, Monitoring Appliances, Available Logs, Use of Virtualization, etc.)
- Consider security in all aspects of legal work; product decisions, contracts, M&A, outsourcing, marketing
- Take into account security when considering an EOL plan
- Supervise effective breach response

Regulator Expectations

- That you will have a plan
- That you will follow your plan
- That you will take information about vulnerabilities (even vulnerabilities in third-party software that you distribute or rely upon) seriously and fix it or warn about it
- That you will stay current with patch management, and with security alerts
- That information security will be an organizational priority
- That you don't "abandon" and fail to support products and services, thus letting security holes exist

Council Expectations – PCI Compliance

- It mandates security processes for handling, processing, storing and transmitting payment card data.
- ALL merchants or merchant service providers that accept, transmit, or store any cardholder data must comply.
- This is a contractual standard. Payment processor contracts and merchant rules bind you to PCI-DSS compliance.
- The PCI-DSS acts as a floor, not a ceiling—many PCI-compliant entities are breached.

Why is compliance important?

- It's the law in some states (i.e., Washington, Minnesota, Nevada and Massachusetts)
- Fines for non-compliance
  - MasterCard: $25,000 – $200,000 depending on # of past violations
  - Visa: $5,000 – $25,000/monthly depending on merchant's level
  - American Express: 0.75% of each non-compliant transaction
  - Discover: $20,000 – $50,000 per violation plus up to $50,000 per month of non-compliance
- Fines for data breaches during non-compliance period
  - MasterCard: $100,000 for each violation of a PCI requirement
  - Visa: $500,000 per incident
- Chargebacks for fraudulent transactions
- Reputational harm
- Costs of investigating, remedying and litigating breaches

PCI-DSS Myths

- A PA-DSS-compliant vendor will make us compliant.
- Our website uses a payment processor gateway plugin – there's no card's stored on our site
- We outsource card processing, so PCI-DSS couldn't possibly apply
- Outsourcing card processing makes us compliant.
- Becoming compliant with PCI-DSS is an IT project.
- PCI-DSS compliance makes us secure
- We don't take enough cards to be subject to the PCI-DSS.

How to Approach Compliance: An Overview

- Assemble the team and require ownership of the issue
- Interview personnel and conduct scans to locate cardholder data in your environment
- Emphasize security and risk, not just security
- Conduct data store analysis: decommissioning, encryption and tokenization
- Implement thoughtful network segmentation
- Implement policy and programmatic changes to your IT standards
- Conduct training and awareness activities

What Can You Do to Enhance Knowledge of "Carding" Your Brand

- Card brands and Merchant Bank Processors already have grey hat hackers that listen to carding forums for their Level 1 Merchants
- Consider if your security team should engage the services of a CyberESI, iSight Partners or others that have carding forums or in-country resources.

“Swiss Cheese” Liability Protection Vendor Management

- Best Practices Vendors and Business Partners
  - Maintain oversight of third parties and understand the security controls your vendors and business partners have in place when allowing them access to your network
  - Insist on security provisions in contracts
  - Ensure contracts with 3rd parties (service providers/partners/vendors) properly protect personal information you allow them to access
  - Ensure subcontractors in your supply chain use the same levels of security and create a policy for screening new suppliers
  - Conduct training for third parties authorized to access your network (and retain documentation of that training)
  - Audit these programs annually

“Swiss Cheese” Liability Protection
Cyber Liability / Breach Insurance

- Coverage is still expensive and the market has not yet matured
- Coverage is caveated by: results from risk management software, underwriting certifications and continuing notice obligations
- Additional endorsements may be necessary to address the entire universe of risk (digital income coverage, cloud computing, digital extortion/ransomware)

ZwillGen PLLC

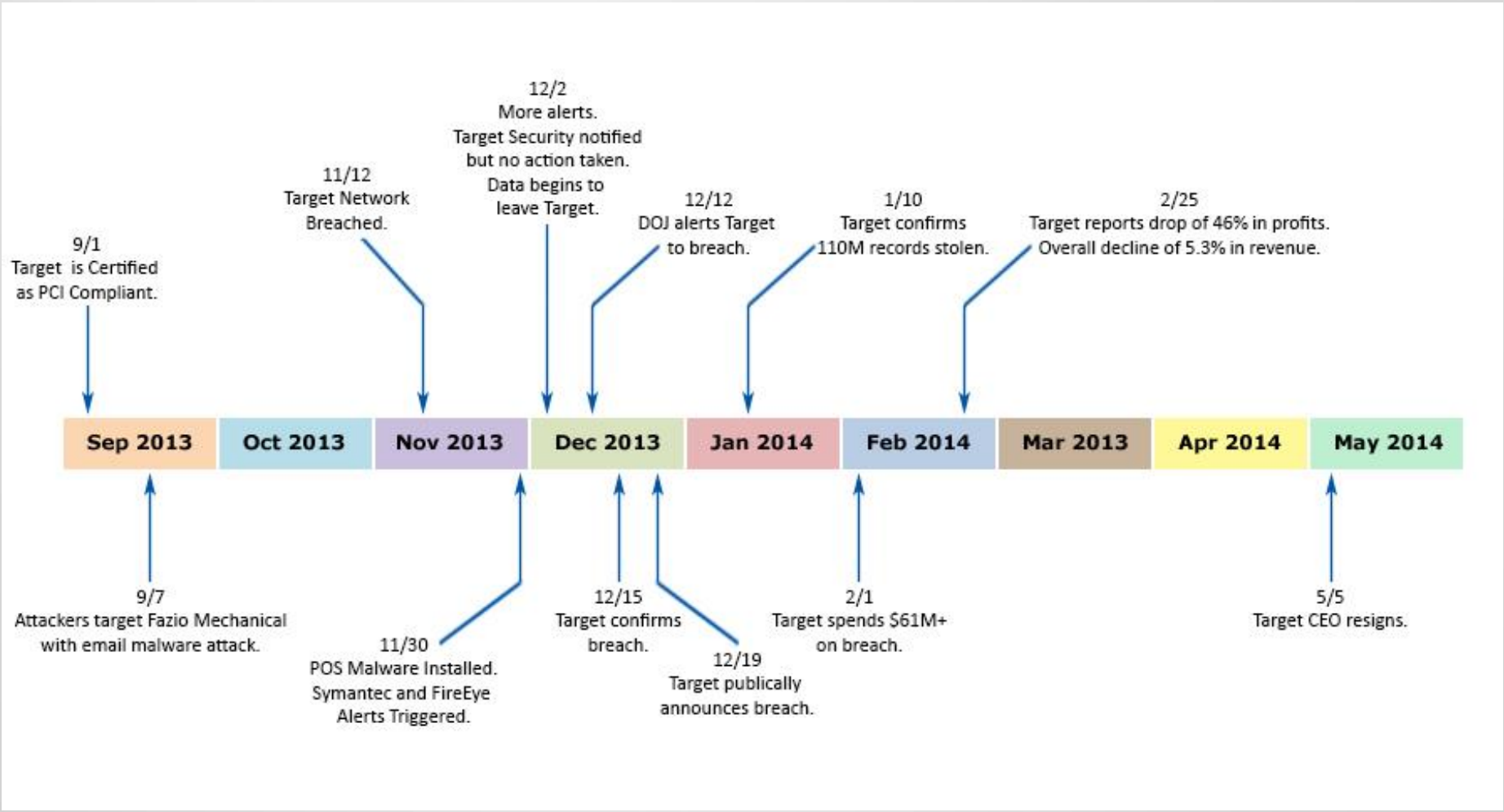
Data Breach Lifecycle: How to Respond?

I've Been Breached: Importance of Effective Response

The future success of a company can depend on how quickly it can stop, respond to, and remediate a breach. Companies can see lasting affects from a breach including:

- Damaged reputation.
- Decrease in stock prices.
- Decrease in profits.
- Change in Leadership
- Lawsuits and/or fines for not complying with Federal and State reporting requirements.

Target: A Timeline



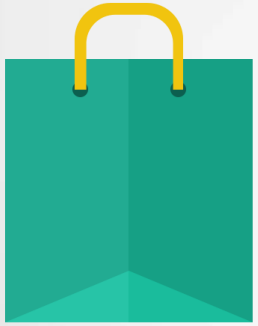
Overview of Effective Response

- Implement your data breach response plan immediately.
  - Call outside counsel
  - Call an incident response firm
  - Preserve data immediately
  - Call your PR organization
  - Determine if and when to contact law enforcement
  - Identify notice reporting obligations and prepare appropriate consumer notices.

Focus on Questions of Legal Significance

- Ensure the investigation stays focused on questions with legal significance.
  - Source and scope of breach:
    - How did the breach occur?
    - What data was compromised?
    - Have we investigated diligently?
    - Have we responded promptly?
    - What, if anything, was damaged or removed?
    - Should we disclose the breach?
    - Should we contact law enforcement?

Notice and Disclosure Requirements



Notice to Consumers

Comply with notice obligations under state and federal regulations

Notice to Business Partners

Comply with disclosure obligations under relevant contracts

Notice to Law Enforcement or Regulatory Agency

SEC requires disclosure of a material incident in filing.

Post-Breach Card Brand Investigation

- Document the following:
  - The facts of the breach and the method of its detection
  - Remediation steps
  - Chain of custody
- Card brands will notify you if hiring a PCI Forensic Investigator (PFI) is necessary.
- The payment card processor or any of the payment card brands may require validation of subsequent PCI compliance and incident remediation by a Qualified Security Assessor (QSA).

Aftermath of Breach

- Prepare for lawsuits and government investigations.
  - Steps you can take:
    - Organize information collected during internal investigation – keep attorneys involved to preserve privilege.
    - Develop legal strategy and marshal facts to counter likely claims, such as negligence, inadequate security, and lack of timely notice.
    - Notify insurance provider to address any coverage issues associated with cost of breach itself and related litigation/investigations.

What about suing the hacker?

- Attribution is very difficult – attackers jump through multiple systems
- Civil litigation is an inefficient way of investigating sophisticated attacks
- Legal process is required for traceback, which can take months to issue, and relevant logs may not exist
- Trails often grow cold overseas - hard to bring suit in “Warlord court” in Nigeria.
- Undercover operations are expensive, ethically challenging and required third parties