

2015 HOSPITALITY LAW CONFERENCE

FEBRUARY 9-11, 2015



ANATOMY OF A HOSPITALITY DATA BREACH

Presented by:

Sandy B. Garfinkel, Eckert Seamans Cherin & Mellott, LLC
&
Lara A.H. Shortz, Michelman & Robinson, LLP

PRESENTERS



Sandy B. Garfinkel

Chair of Data Security & Privacy Group,
Eckert Seamans Cherin Mellott, LLC
sgarfinkel@eckertseamans.com



Lara A. H. Shortz

Hospitality Industry Group,
Michelman & Robinson, LLP
lshortz@mrllp.com



2015 HOSPITALITY LAW CONFERENCE

FEBRUARY 9-11, 2015



ANATOMY OF A HOSPITALITY DATA BREACH

Presented by:

Sandy B. Garfinkel, Eckert Seamans Cherin & Mellott, LLC
&
Lara A.H. Shortz, Michelman & Robinson, LLP

THE DATA THEFT REALITY

- Hackers are ahead of the game; security technology cannot keep up
- Security industry sources:
 - 79% of all companies and organizations in the U.S. have had a data breach in the past two years
- Per one industry source, there have been 696 reported breaches as of 12/1/14, a 26.1% increase over the same time period last year (552)



TARGET TARGETED

December 2013:

- Target Hacked in Pre-Christmas Attack
 - Up to 70 million Target customers affected
 - Customer names, credit/debit card numbers, card expiration dates, debit-card PINs and magnetic strip data
 - Also non-payment card info: phone numbers, e-mail addresses



HOW QUICKLY WE FORGET

Since Target:

- Home Depot
- JP Morgan Chase
- K-Mart



SONY PICTURES

- Blackmail-style threats made concerning release of film “The Interview”
- Hacker infiltrated system, stole and disseminated highly sensitive data
- State sponsored activity? Or disgruntled former employee?



WYNDHAM'S WOES

- **2008, 2009, 2010: *Wyndham Worldwide* suffered 3 separate attacks on its central property management and reservations systems – approximately 45 individual hotels were hit, and about 800,000 credit card accounts were stolen**



THE HOSPITALITY INDUSTRY IS VULNERABLE TO CYBER THREATS



HOSPITALITY ENTERPRISES FACE UNIQUE CHALLENGES

Variety of PII they process and maintain:

Consumer

- Credit/debit card
- Contact information (name, address, phone, e-mail)

Employee

- Social Security Numbers
- Contact information



HOSPITALITY ENTERPRISES FACE UNIQUE CHALLENGES



Unique operational features of their businesses:

- High volume of consumer traffic
- U.S. and international guests
- High employee turnover
- Need to tie into the computer systems of other entities, e.g., franchisors, outside vendors

WHITE LODGING: NETWORKED POS SYSTEM ATTACK

- 2014: Breach at 14 managed properties
- Credit and debit card info stolen via infected POS systems at food and beverage outlets (restaurants, lounges)
- Management company's linked system permitted the malware to spread between properties



MARRIOTT AND FCC: BLOCKING OF PERSONAL WI-FI

- Marriott International blocked personal Wi-Fi signals at Tennessee conference
- Sought FCC ruling legality, citing concerns over data security, among others
- January 2015: Marriott withdrew request after mounting consumer complaints



P.F. CHANG'S: CARD PROCESSING SYSTEMS HACKED

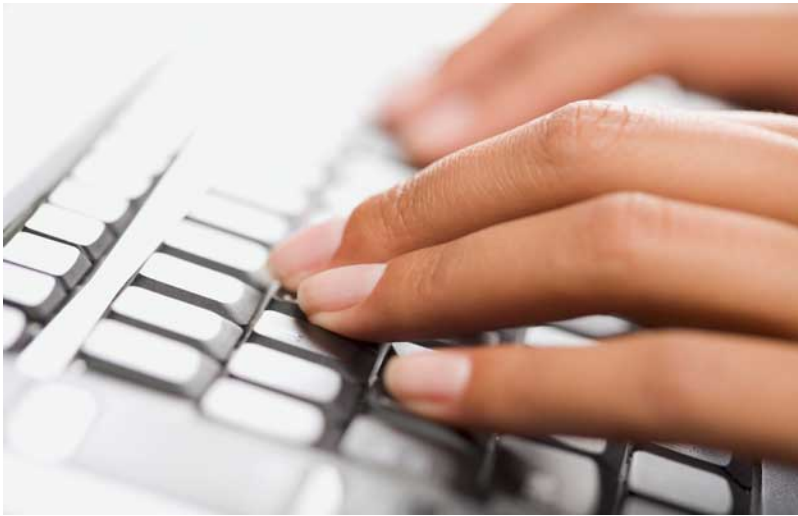


- June 2014: Class action filed for breach at 33 restaurant locations
- Credit and debit card info stolen
- Resulted in company moving to manual credit card imprinting system; established website: pfchangs.com/security
- In December, N.D. III. dismissed action for lack of standing, concluding “possible future injury” is not “actual harm”

GUEST WI-FI: “DARK HOTEL”



- Travelers may be hacked through hotel Wi-Fi networks
- Theft of information from electronic devices through hotel Wi-Fi:
 - “When the guest connects to the hotel’s wireless Internet, he submits his room number and surname. Darkhotel then invites him to download a backdoor that pretends to be an update for legitimate and common software”



- Once on the system, the backdoor can log all keystrokes, hunt for passwords, and collect data about the system.
- The malware can remain on the system undetected for months before going into work gathering data

STATE LAWS GENERALLY CONTROL NOTIFICATION

- **47 States and the District of Colombia have data protection/notification laws**
- **PA Breach of Personal Information Notification Act, 73 P.S. § 2301 et seq.**
- **Congress has been considering multiple proposals for a federal data protection/notification law that may or may not preempt state laws**
- **As to certain specific types of data, federal laws and regs may control notification (e.g., HIPAA, HITECH)**

CHANGING STATE LAW LANDSCAPE

- State Data Breach Notification laws change and evolve
- FLORIDA and IOWA amended their laws in 2014
- Florida:
 - 30 day deadline for notification from determination of a breach or reason to believe a breach occurred



TYPICALLY PROTECTED DATA (“PII”)

Date	Amount
10/20	\$ 738.97
10/21	526.82
10/22	590.53
10/23	524.21
10/24	362.24
10/27	308.42

Credit/Debit Card Account Information (name of cardholder, account numbers, passwords)

- Bank or Financial Account Information (name of cardholder, account nos., passwords)
- Social Security Numbers
- Driver’s License Numbers

PROTECTED ONLY IN CERTAIN STATES:



- Medical Information
- Health Insurance Information
- Biometric Data (fingerprint, voiceprint, retina image)
- Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names
- Digital signatures
- Parent's legal surname prior to marriage

NOT PROTECTED

- Publicly available information that is lawfully made available to the general public from Federal, State or local government records
- Information that an individual has consented to have publicly disseminated or listed (under some state laws only)



PAPER FILES ARE NOT IMMUNE

- *Misconception* that data theft is always a high-tech attack on electronically stored information
- Paper files containing personal information can be just as vulnerable and are often the target of theft
- Some state laws are confined only to addressing electronic breaches, but a few specify that personal information stored in paper form is covered



EMPLOYEE DATA

CO. FILE DEPT. CLOCK NUMBER		Earnings Statement		ADP	
MCB 216543		02470383 0		Period ending: 00/00/0000 Pay date: 00/00/0000	
XYZ Corporation 100 Corporation Crt New Town USA 10000		JANE HARPER 101 MAIN STREET ANYTOWN, USA 12345			
Social Security Number: 999-99-9999 Taxable Marital Status: Married Exemptions/Allowances: Federal: 3, \$25 Additional Tax State: 2 Local: 2					
Earnings	rate	hours	this period	year to date	
Regular	10.00	32.00	320.00	16,640.00	
Overtime	15.00	1.00	15.00	780.00	
Holiday	10.00	8.00	80.00	4,160.00	
Tuition			37.43	1,946.80	
Gross Pay			\$ 452.43	23,526.80	
Deductions	Statutory				
	Federal Income Tax	- 45.22		2,351.44	
	Social Security Tax	- 29.83		1,551.67	
	Medicare Tax	- 6.98		362.89	
	NY State Income Tax	- 17.37		903.24	
	NYC Income Tax	- 8.23		427.96	
	NY SU/SDI Tax	- 0.60		31.20	
	Other				
	Union Dues	- 5.00		100.00	
	401(K)	- 28.85		1500.20	
	Stock Plan	- 15.00		150.00	
	Life Insurance	- 5.00		50.00	
	Loan	- 30.00		150.00	
	Adjustment				
	Life Insurance	+ 13.50			
Net Pay			\$ 273.66		
* Excluded from federal taxable wages					
Your federal taxable wages this period are \$386.66					
XYZ Corporation 100 Corporation Crt New Town USA 10000		Payroll check number: 02470383 Pay date: 00/00/0000 Social Security No. 999-99-9999			
Pay to the order of:	JANE HARPER				
This amount:	TWO HUNDRED SEVENTY-THREE AND 85/100 DOLLARS				\$273.66
SAMPLE NON-NEGOTIABLE VOID VOID VOID VOID AFTER 140 DAYS THIS IS NOT A CHECK					
AUTHORIZED SIGNATURE: <i>[Signature]</i>					
*0 24 70 38 3 * :00 4 330 16 2 7 * 100844840 2*					

PIEDMONT HEALTHCARE SYSTEM BREACH

- Theft of employee information (no patient data)
- Up to 10,000 employees may be affected
- Incidents of fraud/identity theft have been reported



UNIVERSITY OF MARYLAND

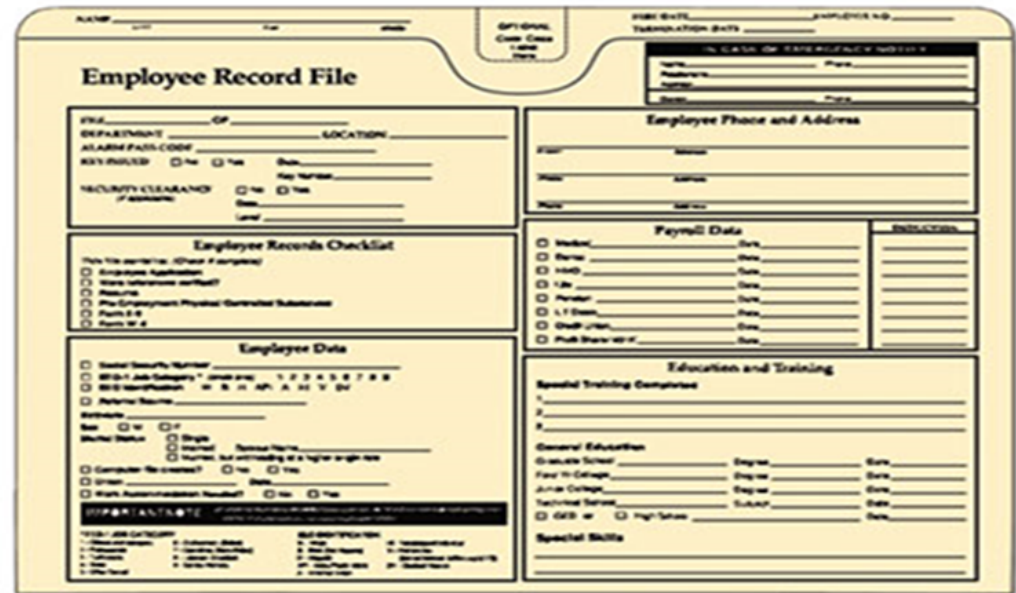
February 2013

- Hackers stole names, Social Security Numbers and birth dates of over 300,000 individuals which included students, faculty and staff



TYPES OF PROTECTED EMPLOYEE INFORMATION

- Personnel File
- Payroll File



The image shows a detailed 'Employee Record File' form. At the top, it includes fields for 'OPTIONAL Case Case Case Case' and 'EMPLOYEE ID'. Below this, there are sections for 'Employee Photo and Address', 'Payroll Data', 'Employee Records Checklist', 'Employee Data', and 'Education and Training'. The 'Employee Data' section includes fields for 'Social Security Number', 'MID Job Category', 'MID Identification', 'Religious Beliefs', 'Marital Status', 'Sex', 'Ethnicity', 'Current No. employees', 'Other', and 'Work Accommodations Needed'. The 'Education and Training' section includes 'Special Training Completed' and 'General Education' with fields for 'Graduate School', 'Four to College', 'Junior College', 'Technical School', and 'GED or High School'. The form also includes a 'Special Skills' section at the bottom.

PERSONNEL FILES

- **Employment Application, which may include:**
 - Name and address
 - Social Security Number
 - Possibly e-mail address
- **Tax forms (W-2, W-4) will have Social Security Number**
- **If employment involves driving, possibly Driver License Number**

PERSONNEL FILES (CONT.)

- Employee Benefit Election Forms
- Social Security Numbers for Employee and Family Members
- Medical Information - may find its way into the file (e.g., workers' comp or disability claim)

The image shows a personnel file folder with a form attached. The form is titled "CONFIDENTIAL Personnel File" and contains the following sections:

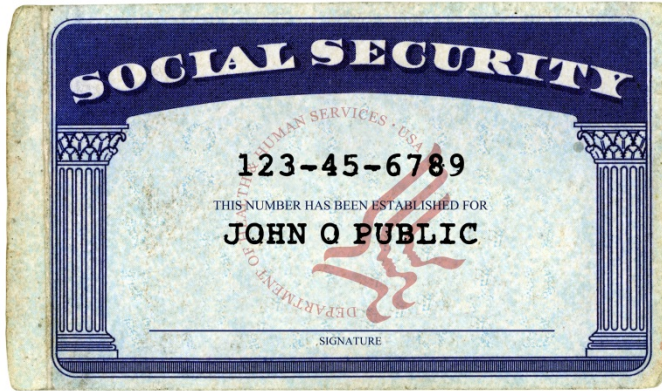
- Employee Information:** Fields for Employee Name (Last, First, Middle, Initial), Employee Number, and Start Date.
- Status:** Radio buttons for Full Time, Part Time, and Temporary.
- Current Address:** Fields for City/State/Zip and Telephone.
- Emergency Contact:** A box labeled "In Emergency Notify" with fields for Name, Telephone, Address, and City/State/Zip.
- Social Security:** A field for Social Security # and a checkbox for "I-9 Documentation completed?" with Yes/No options.
- Education:** Radio buttons for Grade School, High School, and College.
- Special Training:** A field for Special Training.
- Years of Service:** A row of boxes for years 1 through 25.
- Reason for Change or Termination:** A field for Reason for Change or Termination.
- Employment History:** A table with columns for Start/Change Date, Position, Department, and Rate of Pay.

PAYROLL FILE

- Tax forms (W-2, W-4) will have Social Security Number
- Direct Deposit Forms will include Bank Account Information
- If paycard payment system has been adopted, the file might include what would be considered Credit/Debit Card Information



SOCIAL SECURITY NUMBERS



- Industry experts: Social Security Numbers are the most key piece of information exploited by identity thieves
- Social Security Numbers can be used to:
 - File false tax returns
 - Apply for new credit cards
 - Access financial accounts

RESPONSE & NOTIFICATION



WHICH STATE'S LAW APPLIES?

- *The law of the state where the affected individual (cardholder, employee) resides is the law that governs notice – NOT the state where the merchant or employer is situated.*
- This means that **some merchants or businesses may have to comply with *many* state's laws when responding to a single breach**

“BREACH”

Example: PA’s “Breach of Personal Information Notification Act” – defines breach as:

- *Unauthorized access and acquisition of **computerized** data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth.*

“BREACH”

Example: Hawaii “Notification of Security Breaches” law:

- (I) *Unauthorized access to and acquisition of unencrypted or unredacted records or data (computerized, paper or otherwise) where the illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person; OR*
- (II) *Unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key.*



PA BREACH NOTIFICATION ACT - WHEN BREACH OCCURS, WHO MUST ISSUE NOTIFICATION?

- **An entity that maintains, stores or manages computerized data that includes personal information.**
- **A vendor that maintains, stores or manages computerized data on behalf of another entity must notify the entity on whose behalf the computerized data is maintained, stored or managed. The entity on whose behalf the computerized data is maintained, stored or managed must discharge the remaining notice duties.**

THIRD PARTY VENDOR BREACHES

PAYTIME: 2014

- Outside payroll vendor
- Breach potentially compromised every customer account
- Information on both current and former employees
- Names, addresses, Social Security Numbers and other types of info
- Even though the third-party payroll vendor was in possession of the payroll information when it was exposed, the employer is the party responsible by law for issuing notifications to affected employees



WHO RECEIVES NOTICE:

- The individual (employee, cardholder, consumer)
- The entity on whose behalf a vendor maintains, stores or manages the data
- The nationwide credit reporting agencies must be notified; usually this is triggered if more than 1,000 individuals receive notice at one time
- Some statutes require a separate notice and/or copy of consumer notice to be sent to the state attorney general and/or a state consumer protection agency

TIMING

Most state statutes require that notifications must be issued “*without unreasonable delay.*”

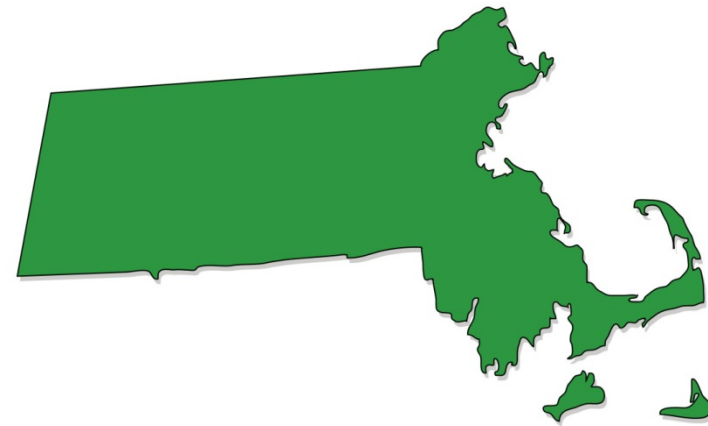
EXCEPTIONS

- Notification may be delayed if a law enforcement agency determines that it will impede a criminal or civil investigation and the agency has so advised in writing. Notification is required after the law enforcement agency determines that it will no longer compromise the investigation or national or homeland security
- Notification may be delayed to determine the scope of the breach and to restore the reasonable integrity of the data

CONTENT OF NOTICE

Massachusetts

- Individual's right to obtain a police report
- How to request a security freeze and necessary information to be provided when requesting a security freeze and any required fees
- Notification (to residents) shall not include the nature of the breach or the number of residents affected by the breach



CONSEQUENCES OF NON-COMPLIANCE

PA:

- The attorney general may bring an action for unfair or deceptive trade practices under the PA Unfair Trade Practice Act & Consumer Protection Law (no private right of action for affected individual)

CA:

- Permits individual cause of action “to recover damages,” also civil penalty for willful or intentional violation of up to \$3,000 per violation



NEW TREND: SAFE DESTRUCTION

- July 1, 2014:
 - **DELAWARE** passed a law governing safe destruction of records containing a consumer's personally identifiable information
- Requires commercial entities to shred, erase, or to otherwise destroy or modify the records to make the personal information entirely unreadable or indecipherable through any means
- Consumers actually harmed by violations of the law may file a civil action and seek treble damages



FEDERAL DATA BREACH LAW?

- Currently several different data breach bills pending before U.S. Congress
- Passage of a federal data breach law may preempt state law – could result in greater consistency: (a) types of data protected, (b) pre-breach security standards and (c) response and notification requirements



PERSONAL DATA NOTIFICATION & PROTECTION ACT

- Proposed by White House Jan. 2015
- Designed to preempt state notification laws except regarding victim protection assistance
- “*Sensitive Personally Identifiable Information*” is much broader than most states’ definition of PII
- FTC primary enforcement authority; FCC and Consumer Financial Protection Bureau would also have roles



INCIDENT RESPONSE PLAN



- **Action Plan– detection, analysis, recovery and post-incident procedures**
- **Employee Policies & Procedures**
 - Limiting who has access
 - Protocols for transferring information
 - Working off-site
 - Confidentiality & Non-Disclosure Agreements and policies

INCIDENT RESPONSE PLAN

- Internal Procedures – detection, analysis, recovery and post-incident procedures
- Internal Resources – security incident response team (SIRT)
- External Resources
 - Legal
 - Security/Forensics
 - Public Relations
 - Law Enforcement

THE END ...?

Not by a longshot.

Stay tuned for:

- More high-profile data breach stories
- More legislative action by states and possibly the federal government
- More cyber threats and more defenses to respond to them



2015 HOSPITALITY LAW CONFERENCE

FEBRUARY 9-11, 2015



THANK YOU

Presented by:

Sandy B. Garfinkel, Eckert Seamans Cherin & Mellott, LLC
&
Lara A.H. Shortz, Michelman & Robinson, LLP