ID Theft: Managing Risk and Controlling Damage

January 21, 2016 Webinar

Mark D. Belongia
Partner, Duane Morris LLP
(312) 499-6717
MBelongia@duanemorris.com

Patricia S. Hofstra
Partner, Duane Morris LLP
(312) 499-0180
PSHofstra@duanemorris.com

Who We Are

- Duane Morris is a full-service law firm with:
- Core strengths in health law, labor and employment, corporate, employee benefits, litigation, banking and e-commerce.
- The #1 growth record of all major law firms in the U.S. through non-merger activities.
- Twenty-seven offices and over 700 attorneys in the U.S. and abroad.

Who We Are

Mark D. Belongia,

Partner &
Vice Chairman of the Bank Industry Group

- **Mark D. Belongia** practices in the areas of business and commercial litigation focusing on matters in the banking, commercial and sports and entertainment areas. Mr. Belongia has represented clients in a wide variety of matters in areas including white-collar litigation, corporate compliance, entertainment and sports law, and insurance law.
- In addition to his litigation work, Mr. Belongia has extensive regulatory experience, encompassing the representation of bank and thrift organizations of all sizes in diverse geographic locations, ranging from money center and regional financial institutions to small community institutions. He has represented bank holding companies, financial service affiliates and their joint venture partners. He has dealt with both state and federal regulators, including the Department of Treasury, Federal Reserve Board, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation ("FDIC"), the Securities and Exchange Commission, the Financial Crimes Enforcement Network and state banking, securities and insurance regulatory agencies.

Who We Are

Patricia S. Hofstra, Partner
Health Law Practice Group
Duane Morris LLP
190 South LaSalle Street, Suite 3700
Chicago, Illinois 60603
(312) 499-0180
pshofstra@duanemorris.com

Former nurse with over 35 years of legal experience representing health care providers. My practice is general healthcare representation, with an increasing focus on billing and payment concerns and corporate medical practice matters, such as contracts, partnership and operating agreements, mergers and acquisitions.

Why This Topic?

- Last year one of our orthopaedic practice clients was notified by the IRS about suspicious activity with respect to a tax refund. The client learned that a fraudulent tax return requesting a substantial tax refund had been filed using his name. We advised the client on the steps to take to protect himself and his practice and the steps to take to reduce the risk of future identity theft or “hack attacks”. Our client suggested this Webinar.

Why This Topic?

Our presentation will cover general identify theft concerns; such as the one our orthopaedic practice client experienced as well as medical identity theft specific to health care providers and patients. We'll leave 15 minutes at the end of the webinar for questions and answers.

So What Is Identity Theft?

- Identity theft, identity fraud or hacking is the acquisition and then fraudulent use of someone else's personal identifying information ("PII"). It is one of the fastest growing crimes in America with an estimated 700,000 victims each year. On average the identity theft takes place 14 months before the victim discovers it.

What Do The Thieves Steal?

- Social Security Numbers
- Driver's license numbers
- Credit card numbers
- ATM cards
- Mail
- Garbage
- Medical information
  - Prescription pads
  - Provider medical identifiers: NPIs, PTANs
  - Beneficiary medical identifiers

What Do Identity Thieves Do With Stolen Information?

- Drain bank accounts
- Run up credit card charges
- Open new utility accounts
- Get medical services
- File tax returns and get refunds
- Give your name and identity to police during an arrest
- Buy bitcoin

What Do Identity Thieves Do With Stolen Medical Information?

- Obtain medical services
- Bill payers for services not rendered
- Obtain prescription drugs
- Bill payers for medically unnecessary services

DuaneMorris

Common Examples of Ways Providers Contribute to Misuse of Medical Identifiers

- Signing referrals for unknown patients
- Signing certificates of medical necessity (CMN) when the service or supply is not medically necessary
- Signing blank forms
- Writing prescriptions for friends and family

Medical Information Misuse Can Result in Penalties For the Provider

- Civil monetary penalties
- Criminal fines and restitution
- Incarceration
- Exclusion from Medicare and Medicaid
- Disciplinary action by licensing board

A Few Examples

- Physician has prescription pads at home, roommate steals them, writes prescriptions for human growth hormone (HGH) for himself, fills prescriptions at Walgreens using health insurance card and sells the HGH on the street. Gets arrested, turns physician in to authorities. Physician gets arrested and also sued by BCBS for insurance fraud.
- Physician signs blank CMNs for home health agency. Gets paid $500 for each signature. Home health agency bills Medicare for services provided to dead patients using physicians signed CMNs. Physician is in jail.

A Few Examples

- Physician writes pain medicine prescription for close friend. Does not bill friend and creates no medical record. Friend allegedly overdoses on prescribed medication. Physician is arrested and handcuffed in his office by DEA in front of patients. Accused of dealing drugs. News media is with DEA at time of arrest and physician's picture is on front page on newspaper. Physician must defend medical license action, DEA action and wrongful death action.

- Physician's ex-wife and former practice manager gets mad and fraudulently bills Medicare for services not rendered. Physician is debarred from Medicare.

Awareness of Medical Identity Problem

- May take years to come to light
- First notice might be a payer audit requesting medical records for patients provider never treated
- Notice from IRS that provider has earned income not reported on tax documents
- Investigation by DEA or Medical Licensing Board
- Visit by FBI

Best Prevention Practices for Providers

- Actively manage enrollment information with payers
  - Watch for billings from old practice locations or new practice locations opened without provider's knowledge
- Monitor billing and compliance processes
  - Be aware of billings in your name
  - Pay close attention to organizations to which billing privileges have been reassigned

Best Prevention Practices for Providers

- Monitor remittance notices and compare with medical record documentation
- Make sure that documentation supports billed services
- Read all documents before they are signed and keep copies
- Document all conversation regarding billing issues
- Report suspected fraud

Best Prevention Practices for Providers

- Control Unique Medical Identifiers
  - Beware of
    - Prospective Employers
    - Referring providers
    - Staff
- Guard prescription pads
  - Check for missing prescriptions
- Encourage patients to review their bills, patients may be able to spot medical identify theft before the provider can

REMEMBER

- Whether staff or a third-party completes the claims process services, the provider whose name is in the chart and on the bill is responsible for the accuracy of the bill. The provider's signature certifies the truth and accuracy of signed and submitted bills.

Promptly Report Medical Identify Theft Concerns To:

- Local law enforcement
- State medical agency
- Federal Trade Commission
- HHS –OIG
- CMS Health and Human Services Regional Office

Best General Identify Theft Prevention Practices

- Carry only what you need, no extra credit cards, no social security card
- Sign all credit cards immediately
- Sign all receipts
- Alert card issuers when statements are not received
- Check credit card and bank statements carefully and immediately upon getting them

Best General Identify Theft Prevention Practices

- Retain copies of receipts to check against billing statements
- Check credit reports for accuracy
- Shred any documents containing personal identifying information
- Do not give personal information or account numbers without confirming the identity of the person requesting the information
- Do not use easily identifiable PINs or passwords

Promptly Report Identify Theft Concerns To:

- Local law enforcement
- Your bank
- Credit card companies
- IRS

Cause of Cyber-attacks?

- Financially-motivated hacks
- Socially-motivated hacks
- Politically-motivated hacks

DuaneMorris

Current State of Cybersecurity

- Underground Markets (Symantec, 2015)

Item	Cost on the Black Market in 2014	Uses
1,000 Email Addresses	$0.50 to $10	Spam and Phishing
Credit Card Details	$0.50 to $20	Fraudulent Purchases
Scans of Real Passports	$1 to $2	Identity Theft
Stolen Gaming Accounts	$10 to $15	Attaining Virtual Items
Custom Malware	$12 to $3,500	Payment Fraud
1,000 Social Media Followers	$2 to $12	Generating Viewer Interest
Stolen Cloud Accounts	$7 to $8	Hosting an Attack Server
1 Million Email Accounts	$70 to 150	Spam and Phishing
Activated Russian SIM Card	$100	Fraud

Current State of Cybersecurity

- Underground Market Prices

	USD	JPY
Visa, American Express, Discover	$4-$8	¥409 - ¥818
Credit Card with track 1 and 2 data	$12	¥1227
Full user information	$25	¥2557
1,000 Infected Computers	$20	¥2046
DDOS Attacks (per hour)	$3-$5	¥306 - ¥511

Current State of Cybersecurity

- Common attack types:
  - Target people (social engineering attacks)
  - Exploit security weaknesses in websites, databases, etc.
  - Exploit systems with missing security patches
  - Denial of service attacks

Current State of Cybersecurity

- Who's launching cyber-attacks?
  - Script Kiddies
  - Professional/skilled hackers
  - Advanced persistent threats

Current State of Cybersecurity

- Who's launching cyber-attacks?
  - Hacker groups
    - Anonymous
    - Cult of the Dead Cow
    - Equation Group
    - Lizard Squad
    - Syrian Electronic Army
    - CyberVor

Current State of Cybersecurity

- Who's launching cyber-attacks?
  - Organized cyber-crime rings
    - Russian and Chinese
  - Lone wolves
    - They operate outside of any command control structure

Current State of Cybersecurity

- Overall, two concerning trends today:
  - The availability of hacking tools is unprecedented
    - Easily buy on the internet
  - Uptick in ransom ware
    - Highly sophisticated and untraceable

Weak/Default Passwords

- Numerous password database breaches in recent years
- Password cracking technology taken to new level with graphic cards processor capabilities
- WiFi used to steal passwords
- Watch yourself in public

Password Reuse and Breaches

- Online banking password with at least one nonfinancial website
- Lack of password complexity
- Same password for several different financial accounts

Six Critical Steps to Take if You Have Been Hacked:

1. Find Out What Happened.

To respond effectively, get a full picture of what happened, including how the hackers got in, which computers and accounts were compromised, which data was accessed or stolen and whether any other parties -- such as customers or business partners -- were affected.

This can be a difficult process involving costly security consultants, but you may be able to get less expensive help from companies you do business with, including your Internet service provider, security software company or website hosting firm. But the best route may be to contact your local, county or state police computer crimes unit and the FBI, which can do forensic analyses and provide valuable guidance.

Six Critical Steps to Take if You Have Been Hacked:

2. Seek Legal Advice.

If you don't have a special cyber-insurance policy that will provide an experienced attorney, you may need to hire one to navigate the legal issues. For instance, when hackers gain access to the personal information of customers or employees, you likely have a legal obligation to notify them.

You may also be required to alert state authorities. Because there isn't a federal data-breach notification rule, companies that do business nationally may have to comply with as many as 46 different state laws. You also could face liability lawsuits from affected parties.

Six Critical Steps to Take if You Have Been Hacked:

3. Communicate Early and Often.

Quick and honest communication with affected employees, customers and partners -- about what happened, what you're doing about the problem and what they need to do -- is often more than just a legal requirement. It may be necessary to salvage your business.

"A data breach can be fatal for a small business" if monetary losses, the cost of rebuilding or reputation damage is high. Maintaining trust in a crisis is the best way to hold onto your customers.

Six Critical Steps to Take if You Have Been Hacked:

4. Eliminate The Problem.

To limit the damage, you may need to take disruptive and costly steps, such as removing infected computers and shutting down your website while you clean up. Consider reformatting hacked computers and restoring data with clean backups, or simply buy new computers.

If hackers exploited a software flaw, apply a "patch" from the software maker that fixes the problem or implement a recommended workaround. If they stole passwords, secure your accounts and set new, complex passwords that will be hard to crack.

Six Critical Steps to Take if You Have Been Hacked:

5. Rebuild.

Put in place the technology and policies to help fend off future attacks. Make sure your computer operating system and other software are current and, if possible, receiving automatic updates to fix bugs. Consider designating one computer for online banking only, meaning no Web surfing and no email that might expose you to malware designed for financial fraud.

Six Critical Steps to Take if You Have Been Hacked:

6. Revisit Your Security Plan.

Make sure your security defenses are running properly and that data is being backed up securely. Your IT manager should consider setting up activity "logging," or tracking, on all devices on your network so any future problems can be investigated more easily.

Check with customers, partners and vendors to see what they're doing to protect your data. Consider buying a cyber-insurance policy if you don't already have one. Also, create a disaster recovery plan and train employees so everyone can respond quickly and calmly if faced with a hack or other crisis again.

DuaneMorris

QUESTIONS?

THANK YOU

Mark D. Belongia
Partner, Duane Morris LLP
(312) 499-6717
MBelongia@duanemorris.com

Patricia S. Hofstra
Partner, Duane Morris LLP
312) 499-0175
pshofstra@duanemorris.com