MINNESOTA LAWYERS MUTUAL
INSURANCE COMPANY

Hacking and Wire Fraud

Tim Gephart
Vice President Claims
Minnesota Lawyers Mutual

Molly Eiden
Claim Attorney
Minnesota Lawyers Mutual

Overview

1. What is a data breach?
2. Technology statistics
3. Why do lawyers need to be aware?
4. How do breaches happen?
5. What data do you need to secure?
6. Steps to combat breaches
7. Regulations
8. Insurance coverage

What is a Data Breach?

Definition: An incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so.

- Data breaches may involve Personally Identifiable Information (PII), trade secrets or intellectual property.

Technology Statistics

Digital Information Explosion!

- 99.9% of new information is stored digitally
- Amount of digital information doubles every 1.5 years
- Every day we create as much information as we did from the beginning of time until 2003
- Google alone processes on average over 2.3 million search queries per second, making it over 11 billion in one single day
- More than half from mobile devices

Source: http://www.internetlivestats.com/google-search-statistics/

Rise in Data Breaches

- **78%** of organizations experienced a data breach in the past two years.
  - **72%** of businesses that suffer major data loss shut down within 24 months
- Estimated that cybercriminals steal **$1 billion** every year from small and medium sized business in the U.S. and Europe.
- **60%** of small to medium sized businesses admit that they do not routinely back up data
- Only **50%** of law firms have encryption and **less than 1/3** use encryption.

2015 ABA Legal Technology Survey Report

Security Statistics

- Over **169 million** personal records were exposed in 2015, stemming from 781 publicized breaches across the financial, business, education, government and healthcare sectors.

  "ITRC Data Breach Reports – 2015 Year-End Totals" | ITRC

- In 2015, there were **38 percent** more security incidents detected than in 2014.

  "The Global State of Information Security Survey 2016" | PWC

- The median number of days that attackers stay dormant within a network before detection is **over 200**.

  "Microsoft Advanced Threat Analytics" | Microsoft

- As much as **70 percent** of cyberattacks use a combination of phishing and hacking techniques and involve a secondary victim.

  "2015 Data Breach Investigations Report" | Verizon

- The majority of data breach victims surveyed, **81 percent**, report they had neither a system nor a managed security service in place to ensure they could self-detect data breaches, relying instead on notification from an external party. This was the case despite the fact that self-detected breaches take just 14.5 days to contain from their intrusion date, whereas breaches detected by an external party take an average of 154 days to contain.

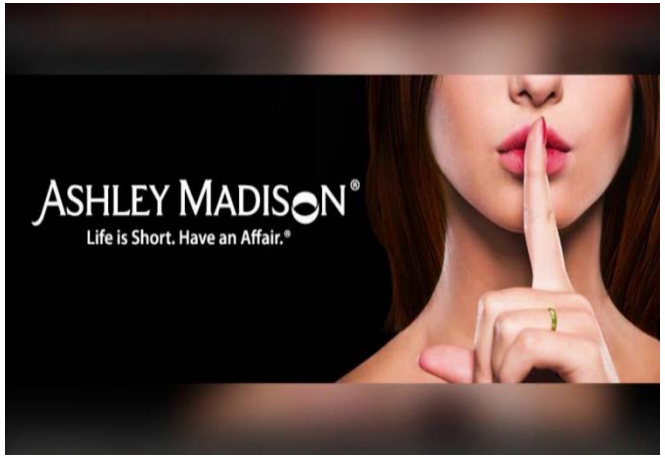
  "2015 Trustwave Global Security Report" | Trustwave

"There are only two types of companies left in the United States according to data security experts: 'those that **have been hacked** and those that **don't know they've been hacked.**'"

Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 360 (M.D. Pa. 2015).

Lawyers and Cyber Security

- Duty to protect client information
- Desire to provide excellent legal service
- New state and federal statutes and regulations
- Client expectations
  - *March 27, 2015: Citigroup report chides law firms for their failure to disclose data breaches. Clients are expecting law firms to have cyber security systems in place.*
- Data breaches make the news



MOSSACK FONSECA

Implications for Traditional Legal Practices

What's easier?

- Hacking into a highly secure financial firm to access sensitive data

OR

- Finding a lawyer's cell phone left in a coffee shop containing highly sensitive emails from that same financial firm?

Who has access to a lawyer's data?

- Litigation support
- Transcription
- Off-site storage
- Accountants
- Disaster recovery back up tapes/archives
- Mail room/courier/photocopy/shredding services
- Cleaning service

Cloud Storage

Easier access for you

=

Easier access for them

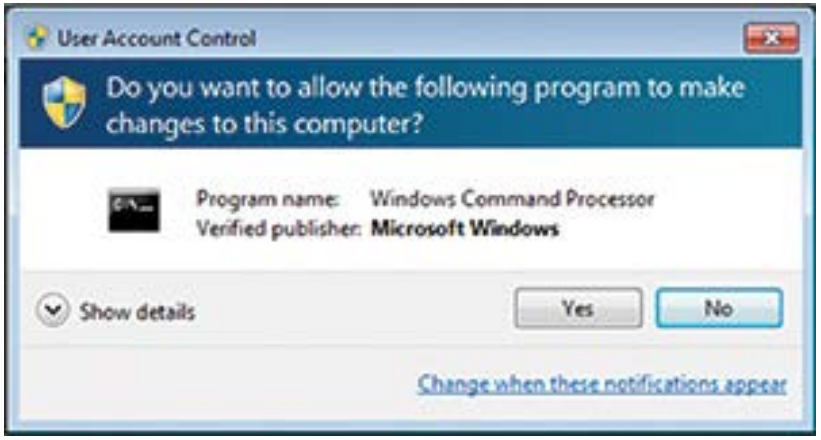
How do breaches happen?

- **Social Engineering**
  - Obtaining sensitive information by trickery, often using information obtained from social media
  - Very easy for criminals

- **Theft by Individuals with Access**
  - Employee
  - Vendors
    - Outsourced IT
    - Cleaners
    - Accountants/Consultants/Experts

- **Hacking**

Common Hacking Technique



- Hackers often employ an authentic-looking Microsoft Windows "User Account Control" message box to lure users into giving permission to allow the "Windows Command Processor" to modify the user's computer settings.

Who are the hackers?

- Operations in China, Eastern Europe, Africa
- Domestic operations
- State sponsored clandestine operations

Fake Ethics Complaint Scam

- A new internet scam is targeting lawyers by exploiting one of their great fears: getting slapped with a disciplinary complaint.
  - The emails, which typically appear to originate with a state bar association, come with a subject line informing the recipient that they are the subject of an ethics complaint, which is supposedly attached to the email. The email address is spoofed, the attachment contains ransomware, and any lawyer who clicks on it is up the proverbial creek without a paddle.
  - For those unlucky lawyers who let down their guard, ransomware poses ethical and practical dilemmas for which there are few obvious answers: "Do I pay the ransom? What happens if I can't get my client data back? What do I do for my clients? Do I have to notify them?"

Mike Mosedale. "Ransomware scam targets lawyers with phony ethics complaints."
Minnesota Lawyer. 7 July 2016: Email newsletter.

MINNESOTA LAWYERS MUTUAL
INSURANCE COMPANY

Fake Wiring Instruction Scam

LAWYERS MUTUAL

RISK MANAGEMENT ALERT

WEBSITE | YOUR POLICY | RISK MANAGEMENT | CLE | CLAIMS | ABOUT US

May 2016

NC State Bar Scam Warning from Peter Bolac

DON'T BE A VICTIM OF WIRE INSTRUCTION FRAUD

Hundreds of thousands of dollars are being scammed from law firms because of fake wire instructions.

You can prevent this fraud through the use of secured email.

1. Always use a secure domain. Email services such as AOL, Gmail, and Yahoo are easy targets for hackers.
2. Check email addresses for accuracy. In many cases, a fraudulent email is close, but not the correct address.
3. Do not accept changes in wiring instructions made via email.
4. All wiring instructions should be verified, preferably in person or by a telephone call that you initiate using contact information from your file (not from an email that may be fraudulent).
5. Here is a sample disclaimer to use when you transmit wiring instructions:

IF YOU RECEIVE **NEW** WIRING INSTRUCTIONS ON THIS TRANSACTION
PLEASE NOTIFY ME IMMEDIATELY
THE SMITH JONES LAW FIRM **DOES NOT** ALTER ITS WIRING INSTRUCTIONS

STAY CONNECTED

Join the mailing list

Lawyers Mutual | social@lawyersmutualnc.com | www.lawyersmutualnc.com
Post Office Box 1929 Cary, NC 27512

Click to view video: https://www.youtube.com/watch?v=mgI_QX1oK6E

MLM Claim Example

- Attorney represented the buyers in the purchase of a home. Attorney e-mailed them with instructions on where to wire the $30,000 for the closing. Days later, the buyers received different wiring instructions. A hacker had infiltrated the attorney's email system and had sent the fraudulent wiring instructions to the buyers. About $16,500 of the money was gone, but the bank held on to $13,500, which it would not release without a court order.

- The buyers ended up recouping their money from the bank.

"The Panama Papers"

- **Mossack Fonseca**
  - Largest known data breach in history
  - The leaked information allegedly details the ways dozens of high-ranking politicians, their relatives or close associates in more than 40 countries, including the U.K., France, Russia, China, and India, have used offshore companies to hide income and avoid paying taxes.
  - The leaks reportedly cover **11.5 million** confidential documents dating from the 1970s through late 2015. The 2.6 terabytes of leaked data include 4.8 million emails, 3 million database format files, 2.2 million PDFs, 1.1 million images, and 320,000 text documents.
  - Attackers may have compromised the Mossack Fonseca network and elevated privileges to that of a domain administrator or email administrator and used these elevated privileges to access and download all the data contained on the e-mail server.

Watering Hole Hack

- In 2012, the law firm Fried Frank was hacked using a “watering hole” technique.
  - Hackers analyzed the employee web traffic and set up fake websites that mimic their favorite webpages. The employees entered passwords, which were then viewed by the hackers. The employees were using the same passwords for their personal accounts as they were for their highly secure accounts.
  - While watering hole attacks are uncommon, they pose a considerable threat since they are difficult to detect and typically target high-security organizations through their low-security employees, business partners, connected vendors or an unsecured wireless network.

More Law Firm Hacks

- **February 2012**: Anonymous stole 2.6 gigabytes of e-mail belonging to Puckett Faraj, a law firm that represents Staff Sgt. Frank Wuterich, who pled guilty to leading a group of Marines in Haditha in a 2005 raid, which resulted in the deaths of 24 unarmed Iraqi civilians.
- **2011:** Covington & Burling and other firms were hacked by Chinese. The purpose of the attack was to learn more about the law firm's prominent corporate clients given its work for military contractors and energy companies, including its work on several solar energy projects at the time.
- **March 29, 2016:** Hackers broke into the computer networks of some of the most prestigious law firms. The firms include Cravath Swaine & Moore LLP and Weil Gotshal & Manges LLP, which represent Wall Street banks and Fortune 500 companies in everything from lawsuits to multibillion-dollar merger negotiations.

Bellingham Bank Case

Bellingham, a small bank in Minnesota, obtained insurance from BancInsure, Inc for various circumstances including a "computer systems fraud" provision. Bellingham had a dedicated laptop for a special connection to the Federal Reserve's FedLine system. In order to complete a wire transfer on the laptop, the bank would sign in using three separate passwords. In 2010, an employee unintentionally downloaded the Zeus virus that collects information and sends it back to the hacker. At some point later, a USB with passwords on it was left connected to the laptop overnight and it transmitted the passwords to the hacker. One morning, an employee noticed that $485k had been transferred. Bellingham filed a claim with BancInsure under their policy but BancInsure denied coverage claiming it was an employee caused loss. Bellingham argued that the hacker caused the loss, which would be covered.

- *State Bank of Bellingham v. BancInsure, Inc.*, No. 13-CV-0900 SRN/JJG, 2014 WL 4829184, at *7-8 (D. Minn. Sept. 29, 2014), aff'd, No. 14-3432, 2016 WL 2943161 (8th Cir. May 20, 2016)

Bellingham Bank Factors Analyzed

- The FedLine computer was used for email and personal activity such as web browsing.
- The Administrator and FedLine user accounts on the system were not password protected.
- Symantec Antivirus was configured to warn the user of threats.
- Symantec Antivirus “Proactive Threat Protection” was disabled.
- User activity resulted in the download and execution of the Zeus virus.
- Symantec Antivirus notified the user of the Zeus infection on October 13, 2011 and October 18, 2011. The computer remained in use after these warnings.
- Symantec Antivirus failed to remove the persistent Zeus Trojan in a timely manner.
- Multiple viruses exist on the system.

'Chewy 123': FBI's most-wanted cybercriminal used cat's name as password

November 15, 2014

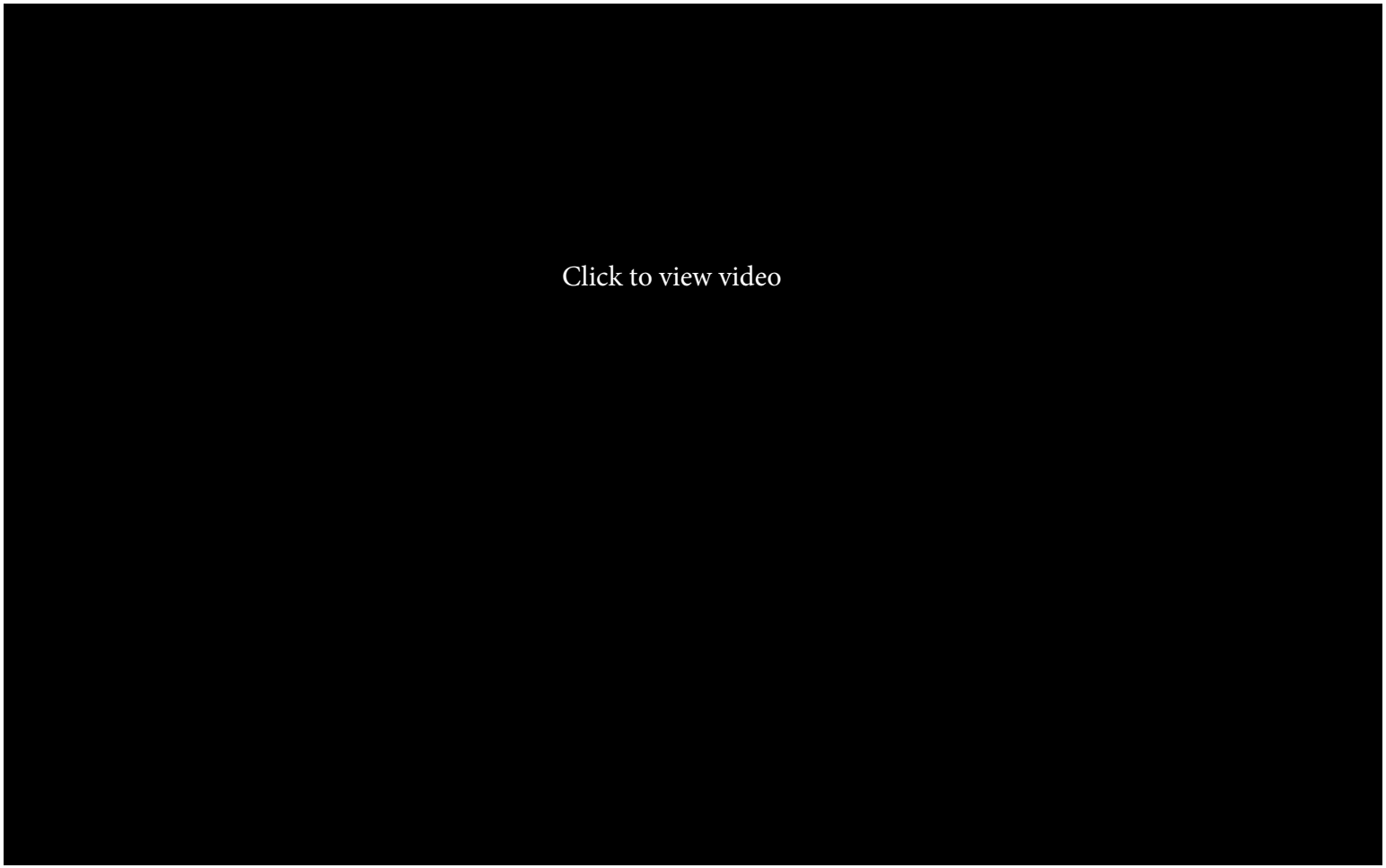
Martha Mendoza

Once the FBI's most-wanted cybercriminal, Jeremy Hammond is serving one of the longest sentences a US hacker has received — 10 years, the maximum allowed under his plea agreement. But to this day, he's unsure how agents cracked his Mac's encryption. Perhaps it was the fact his password was his cat's name and the numbers 123.

Jeremy Hammond was put in prison for 10 years over high-profile cyber attacks. *Photo: Cook County Sheriff's Department*

MINNESOTA LAWYERS MUTUAL
INSURANCE COMPANY

What happens when you dare expert hackers…



What data do you need to secure?

- Client information
  - Personally Identifiable Information
  - Personal healthcare information
  - Sensitive business information: intellectual property, and insider information
  - Bank accounts for wire transfers
  - Credit card information

- Employee information
  - Payroll and benefits information

Practice areas that may elevate exposure

- Securities - data in preparation for securities filings/registration, “quiet period” restrictions on release
- Taxation - financial information
- Trusts and Estates - high net worth client data
- Family Law – financial information

Steps for Combating Data Breaches

1. **Anticipate** –Catalog all confidential data owned or maintained by the firm and ensure that proper security procedures are in place for keeping it safe. Conduct ongoing risk assessments, invest in security measures, and test the integrity of your system on a regular basis.
2. **Train** – Inform employees and vendors of proper security procedures and update policies regularly.
3. **Prevent**
   - Use strong passwords of at least 12 characters and change them regularly.
   - Computers, especially laptops that leave the office, should be protected with whole disk encryption
   - Consider a standardized desktop with firm issued software only.
   - Make sure all critical patches and updates are downloaded.
   - For remote access, use a Virtual Private Network (VPN) or other encrypted connection.
   - Do not let employees use the same password for their personal use as they do for work.
   - Hire an independent security expert to give you an analysis of your system.
4. **Organize** – Form a breach response team and periodically test your breach response. Revise as warranted

Avoiding Common Mistakes

1. Implement a cyber security program.

- Incorporate some common elements, such as anti-virus protections, firewalls, secure connections and require passwords for mobile or desktop devices.

2. Adopt a robust incident response plan.

- Design a response plan before a breach occurs. This may help defend against any claims of negligence should a breach occur.

3. Test the systems.

- Review records and activity logs to determine a baseline for what activity is “normal”. Most hacks, malware or phishing emails do not alert you: “You have been compromised.” More often, evidence of a hack if more subtle. Sometimes the impact is noticed (i.e. money missing from an account) but notice of the breach is not noticed.

4. Train Employees.

- Recognize what some risks look like, what the firm’s security policies are, and how to report a suspected breach. May consider whether certain information, programs or files should be limited to specific employees to reduce the risk of inadvertent disclosures, loss or an internal incident.

Services to Mitigate Cyber Threat Exposure

- **1password**

Download this program and browser add-ins to keep all of your online passwords extra secure. (Just make sure to keep your master password for the program secure). Similar services include Fastpass, Keypass, and Dashlane.

https://1password.com/

- **Windows 10**

Microsoft's new operating system allows easy full disk encryption (no encryption means that anyone can pull the disk out and connect an SATA cable to another computer and remove all of the stored data.)

- **RSA**

A thumb drive sized device gives a new randomly generated pin every 90 seconds. You add the pin to the end of your password.

https://www.rsa.com/en-us

Rules, Regulations, Common Law Actions, and Statutes

- Rules of Professional Conduct
- Federal Regulations on Data Protection and Breach Response Requirements
- Common Law Actions
- Statutory Claims

Minnesota Rule of Professional Conduct Rule 1.1 Comment 8

Maintaining Competence

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, **including the benefits and risks associated with relevant technology**, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

(Emphasis added)

Minnesota Rule of Professional Conduct
Rule 1.6 Comment 17

Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

Rule 1.6, Comment 17 continued

Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.

Minnesota Rules of Professional Conduct
Rule 1.6, Comment 18

When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

Federal Regulations on Data Protection and Breach Response Requirements

- **F.A.C.T.A. "Red Flag" Rule:** Rules that require financial institutions and creditors to develop and implement written identity theft prevention programs.
- **H.I.P.A.A. Security Rule:** Requires appropriate administrative, physical and technical safeguard to ensure confidentiality, integrity and security of electronic protected health information.
- **H.I.T.E.C.H. Law:** Extends the scope of HIPAA requirements to the business associates of covered entities. This also expands the regulations to include mandatory breach notifications, heightened enforcement, increased penalties and patient rights.
- **Gramm-Leach-Biley Act:** Requires financial institutions to have in place standards which protect the security of the their banking customers' nonpublic information.
- **I.T.E.R.A.: The Identity Theft Enforcement and Restitution Act: A**mends the federal criminal code to authorize criminal restitution orders in identity theft cases.
- **Executive Order of February 2013:** Requires several industries to comply with federal data breach notification requirement.
- **Executive Order of April 2015:** Allows the government to impose penalties on foreign individuals or entities that engage in cyber-attacks that threaten U.S. national security or the economy. Penalties include freezing assets or barring commercial transactions.
- **International Reporting Requirements:** The European Union has a data breach notification incentive that imposes steep fines for failure to notify in the event of a breach.

Common Law Actions

- Malpractice
- Negligence
- Breach of fiduciary duty
- Fraud

Negligence

- Duty to take reasonable steps to protect sensitive information provided with belief that the information would be kept secure.

- Failed to take commercially reasonable steps to protect the sensitive information.

- Failure to protect the information resulted in the breach.

Statutory Claims/Consumer Protection Laws

- Communications/web site privacy policy or other materials viewed or received by plaintiff caused plaintiff to believe that his/her information would be kept private

- Plaintiff was misled, provided the information, and was deceived because the information was not kept private

  - Frequently sought because a prevailing plaintiff recovers treble damages and attorneys' fees

Cyber Security Insurance

- Purchase a cyber security policy
- Don’t assume it will be covered by an existing insurance policy
- Cyber liability insurance is designed to respond to losses from a variety of cyber-incidents, including data breaches, network damage, and cyber-extortion.
- Stand-alone cyber liability insurance policies addressing both first- and third-party perils offer a full range of coverage that is key to mitigating risk.
  - **First party losses** – often referred to as “breach responses” coverage, typically covers the costs and expenses incurred in responding to, investigating, and remedying a breach incident.
  - **Third party losses** – the third party cyber liability insurance agreement covers losses arising from claims made against the firm, its directors, officers, and/or employees for the unintentional breach, damage, media liability, and costs associated with regulatory proceedings.

Taking reasonable steps now can save time, money, and embarrassment later.

Questions? Comments?

Tim Gephart

Vice President, Claims

Minnesota Lawyers Mutual Insurance Company

tjg@mlmins.com

612-373-9654

Molly Eiden

Claim Attorney

Minnesota Lawyers Mutual Insurance Company

meiden@mlmins.com

612-373-9643