

# **Cyber Crime and Cyber Security:** **A White Paper for Franchisors, Licensors, and Others**

*Bruce S. Schaeffer, Henfree Chan  
Henry Chan and Susan Ogulnick*



Wolters Kluwer Law & Business is a leading provider of premier research products and tools in many legal practice areas, including a comprehensive suite of products designed to provide the most up-to-date and current information in franchise and distribution law.

The *CCH Business Franchise Guide*, commonly referred to as the “bible of franchise law,” is the only single source of federal and state franchise and distribution laws, regulations, uniform disclosure formats, explanations, and full-text case reporting. It contains the two official formats franchisors use to create presale disclosure and registration documents — the FTC franchise disclosure format and the Uniform Franchise Offering Circular. It includes full-text of state franchise disclosure/registration and relationship/termination laws, state business opportunity laws, and English translations of international franchise laws and regulations. The publication contains a unique collection of more than 6,500 court and administrative decisions (including relevant international decisions), many available only in the Guide. Online customers also have access to a multi-jurisdictional research tool, the Smart Chart™ that compares State Disclosure/Registration Laws, State Relationship/Termination Laws, and State Business Opportunity Laws.

*CCH Franchise Regulation and Damages* by Byron E. Fox and Bruce S. Schaeffer is the first franchise treatise that converts liability into damages and dollars. This valuable work explains franchise law, computation of damages, assessing litigation risks, how to value franchises, and how to use expert witnesses. This resource reviews topics seldom covered in franchise law research, while going directly to the heart of franchise disputes. Bruce S. Schaeffer—noted attorney in the areas of franchising, estate planning, taxation, and securities fraud and founder of Franchise Valuations, Ltd.—has filled this treatise with practice-proven tips. The text also includes thousands of references to laws and cases with linking to the *Business Franchise Guide* for Internet subscribers of both publications.

The franchise and distribution law suite of products is within the Trade Regulation product group. Other CCH reporters in this group are:

- *CCH Advertising Law Guide*
- *CCH Privacy Law in Marketing*
- *CCH Product Distribution Law Guide*
- *CCH Sales Representative Law Guide*
- *CCH Trade Regulation Reporter*

Also look for these soft cover books:

- *FTC Disclosure Rules for Franchising and Business Opportunities, Released January 23, 2007 from the CCH Editorial staff, David J. Kaufmann, and David W. Oppenheim.*
- *International Franchising in Emerging Markets: Central and Eastern Europe and Latin America* by Dianne H. B. Welsh and Ilan Alon, Editors
- *International Franchising in Emerging Markets: China, India and Other Asian Countries* by Ilan Alon and Dianne H. B. Welsh, Editors
- *International Franchising in Industrialized Markets: North America, The Pacific Rim and Other Countries* by Dianne H.B. Welsh and Ilan Alon, Editors
- *International Franchising in Industrialized Markets: Western and Northern Europe* by Ilan Alon and Dianne H.B. Welsh, Editors
- *Master Franchising: Selecting, Negotiating, and Operating a Master Franchise* by Carl E. Zwisler

For CCH publications, visit the online store at [www.business.cch.com](http://www.business.cch.com), or call 800.344.3734.



## Introduction

The history of crime and crime prevention has been akin to the history of warfare: an offense is developed, then a defense counters the offense, then a new offense counters the new defense. Machine guns led to the development of tanks which led to the development of rocket propelled grenades, etc. When commerce consisted of camel caravans, people in the Arabian Peninsula promoted banditry, ultimately forcing the commerce to go by sea. When merchants used the sea lanes through the Mediterranean, the people of the Maghreb promoted the Barbary pirates until they were ultimately countered by a punitive US military action.

More recently, with the advent of the railroads came Jesse James, countered by the Pinkertons and so on. Airlines discovered airline hijackers and parried the threat with the excruciating experience they call airport security. Move followed by counter-move. In the present conditions of economic crisis with thousands of recently fired, super-computer-savvy techies on the loose, the venue for those of dishonest bent is the cyber-world. The newest bandits are the malicious professional “hackers” who are not only well organized but will strike with proven military precision driven by monetary gain. Thus, businesses must learn to be en garde and protect their cyber property, such as Intellectual Property (IP), which frequently accounts for 70% of the market value of companies that specialize in franchising and licensing.

The commonly accepted definition of cyber security is the protection of any computer system, software program, and data against unauthorized use, disclosure, transfer, modification, or destruction, whether accidental or intentional. Cyber attacks can come from internal networks, the Internet, or other private or public systems. Businesses cannot afford to be dismissive of this problem because those who don’t respect, address, and counter this threat will surely become victims.

## Where’s the risk?

Everywhere: Cyber-crime is on the rise. On average, there has been a reported cyber-security event every single day since 2006. If there’s a transaction that involves a card with a magnetic strip and a swipe, there’s a transaction that involves a risk. And if there’s a computer system with software designed to allow access by multiple users (e.g. by franchisees, vendors, or other providers) without security in mind, then there’s a major risk of being hacked for malicious or competitive purposes. Mobile devices, often containing sensitive data, are lost or stolen every day.

Face it: With the proliferation of free hacking tools and cheap electronic devices such as key loggers and RF Scanners, if you use e-mail or your company’s systems are connected to the Internet, you’re being scanned, probed, and attacked constantly. This is also true for your vendors and supply chain partners, including payment processors. E-mail and the web are the two main attack vectors used by hackers to infiltrate corporate networks.

So, clearly, every company is vulnerable because every company needs to have these functions. Conversely every company needs to guard its systems against unauthorized access through these openings because supposed firewalls offer no protection whatsoever once a hacker has entered.

## Who's been hacked?

As they say in the cyber security world, there are only two kinds of computer systems: those that have been hacked and those that will be hacked. For example, crooks used sophisticated methods to evade detection and place malware on nearly 300 Hannaford Bros. supermarket servers to intercept payment information. As many as 4.2 million credit and debit card numbers may have been exposed. Ironically, Hannaford was notified of its massive problems on the very same day it was recertified as being Payment Card Industry Data Security Standard-compliant. *Like an AIDS test, penetration testing in the cyber security arena offers assurance and protection only as of the date of the testing.* So once is not enough. Penetration testing must be done regularly and thoroughly to maintain its value or it becomes worth no more than a cancelled subscription.

And just because people are computer savvy does not mean their data are safe. The website of online retailer Geeks.com featured the “hacker safe” notification from McAfee ScanAlert. Nevertheless, a hacker broke in and accessed customer credit card numbers and other personal information on its site. And in another really scary example, mortgage giant Fannie Mae narrowly avoided a software time-bomb set to destroy all data on its computers. Some disgruntled contractor who had been terminated embedded into the system a malicious code, tucked at the end of a legitimate software program scheduled to run each morning. It was set to go into effect (months after he was gone) on all 4,000 of the company's servers. It was only discovered by chance by another Fannie technician or the whole agency's database would have been wiped out.

Even Deborah Platt Majoras, Chairman of the Federal Trade Commission from 2004 to 2008, was a victim of identity theft. So it's no wonder that she and the FTC have been such strong proponents of protecting consumers from shoddy data protection practices and enforcing regulations and levying fines on businesses.

## What could happen?

Lots of things: all of them bad. Accordingly, a company (particularly franchise businesses and other licensors) must evaluate its risk to determine and implement appropriate policies and procedures.

We have formulated a “Chan Scale of Cyber In-Security”<sup>©</sup>, based on the potential harm that can be caused:



**1 Chan – Low risk.** Hacker has gained entry to system but minimally. Minor risk of business disruption, but access can aid attackers in information gathering and planning future attacks.



**2 Chans – Medium Risk.** Malware has been implanted in the company’s network, which could cause malfunctions and mischief. There is a significant risk of a business disruption that could result in financial loss and/or damage of goodwill.



**3 Chans – Medium-to-High Risk.** Using sniffers or other equipment, hackers have obtained personally identifiable information (PII) from point of sale (POS) systems. There is a significant risk of a business disruption that could create financial loss and/or damage of goodwill.



**4 Chans – High Risk.** Inside job: data stolen by disgruntled employee. There is a potential risk of business disruption, resulting in financial loss and damage of goodwill. PII may be taken, as well as company’s confidential information and financial information.



**5 Chans – Critical Risk.** Hackers have gotten into the system and can access PII as well as the company’s financial information and confidential information. There is a severe risk of business disruption, financial loss, damage of goodwill. System, application, and database have been compromised.

## What are potential liabilities?

Major liability may be incurred from, *inter alia*, individual litigation, class litigation, regulatory investigation, contract dispute, loss of customers, reputation damage, data theft, denial of service, cyber-terrorism, cyber-extortion, and fraud.

***Some statutes impacting cyber-liability include:***

- Communications Act of 1934, updated 1996
- Computer Fraud & Abuse Act of 1984
- Computer Security Act of 1987
- Economic Espionage Act of 1996
- Electronic Communications Privacy Act of 1986
- Federal Privacy Act of 1974
- Health Insurance Portability & Accountability Act of 1996
- National Information Infrastructure Protection Act of 1996
- U.S.A. Patriot Act of 2001
- Payment Card Industry Data Security Standard (PCI DSS) effective 2006 – industry-defined standard, not government

***Introduced in 110<sup>th</sup> Congress (2007) – none enacted:***

- Personal Data Privacy and Security Act of 2007
- Data Accountability and Trust Act
- Identity Theft Prevention Act
- Data Security Act of 2007

***Introduced in 111<sup>th</sup> Congress:***

- S.139, Data Breach Notification Act

**What about policies/procedures?**

Participants at the Davos conference on the international economy that ended in February 2009 took note of the world-wide gangs and other criminal organizations invading the cyber world. They estimated the damages from cyber crime to be \$1 trillion per year. The cost of notifying customers alone in the case of a cyber event has been estimated at \$1-3 per file accessed and \$100-300 or more per file compromised.

In light of these numbers, companies are well advised to have policies in place with respect to data protection, data retention, data destruction, privacy, and disclaimers to customers. And, if a security breach occurs, the company should expect, and be prepared for, a regulatory investigation during which the company will have to show that its policies were well documented, updated as business processes change and *observed*, or risk significant fines, agency oversight, or worse. The policies must be more than mere window dressing; failure to conform to a company's own stated, internal policies may be worse than having no policies at all.

For example, the FTC recently went after two companies for failing to provide reasonable and appropriate security for sensitive consumer information, leading to identity theft and forced a settlement containing bookkeeping and record-keeping provisions to allow the agency to monitor compliance. Under the terms of the settlement, the FTC ordered the two companies to hire third-party security auditors to assess their security programs on a biennial basis *for the next 20 years*; to certify that the companies' security programs meet or exceed the requirements of the FTC's orders; and to prove that the companies are providing "reasonable assurance that the security of consumers' personal information is being protected."

A similarly onerous set of conditions was imposed in February 2009 by the FTC as part of a settlement with CVS Caremark, requiring that company to establish policies for protecting and properly disposing of personal information, to be subject to a biennial audit by a third party, *and to pay a multi-million dollar fine* for improper treatment of information required to be protected under HIPAA.

### **What about cyber crisis planning/management?**

IT (Information Technology) systems are vulnerable to a variety of disruptions from a variety of sources such as natural disasters, human error, and hacker attacks. These disruptions can range from mild (e.g. short-term power outage, hard disk drive failure) to severe (e.g. equipment destruction, fire, online database hacked). Crisis (and Disaster Recovery) planning refers to those interim measures needed to recover IT services following an emergency or system disruption. Interim measures may include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or the performance of IT functions using manual methods to minimize the business impact.

In January 2009 Heartland Payment Systems, which processes 100 million credit and debit card transactions per month, disclosed that hackers had penetrated its computer network. By installing malicious software, the hackers gained access to digital information encoded on a card's magnetic strip that could be used to create duplicate cards. In the wake of what was described as the biggest single breach of consumer and financial data security ever, Heartland's stock was hit hard. In public statements following the incident, Heartland's CEO compared the potential industry-wide impact of the breach to the Tylenol poisonings that nearly brought down the drug maker Johnson & Johnson in the early 1980s.

The Heartland debacle highlights the potential fallout companies face as a result of ineffective planning for data security breaches. The costly consequences may include damage to reputation and brand value, shareholder derivative suits, directors' and officers' liability, regulatory agency investigations, and class-action litigation.

Effective crisis planning and crisis management processes must be developed to enable businesses to continue operating following failure of, or damage to, vital services or facilities.

*The cyber crisis planning process covers the following:*

- Identification and prioritization of critical business processes including the technology that supports them (servers, databases, applications) and technology owners.
- Identification and agreement with respect to all responsibilities and emergency arrangements for business continuity planning and recovery with all affected parties throughout the organization.
- ‘Call Tree’ and contact details.
- Documentation of workarounds (electronic and manual) and/or rectification procedures and a linkage to any relevant reference material or documents.
- Appropriate education of staff in the execution of the agreed emergency procedures and processes.
- Checklists and procedure guidelines to assist all parties to recover from a crisis or disaster.
- Testing and updating of the plans on a regular basis.

*Cyber Crisis Management (Incident Response – Stop the bleeding) process covers the following:*

- **Identify the Crisis at Hand** – For example, is it a customer data breach, privacy breach, virus outbreak, targeted malicious code attack, denial of service attack, phishing attack, or third party data compromise?
- **Analysis and Assessment** – Triage of the incident to determine the severity (See Chan Scale of Insecurity) and impact on the business.
- **Coordination/Response Plan** – Decide whether to protect or prosecute including contacting the proper law enforcement authorities. If prosecution is the course of action, all evidence (system/application logs, audit trails, and affected systems) must be collected in a forensically sound manner to hold up in a court of law. Contact all affected parties and communicate and agree upon a response plan.
- **Containment/Recovery Plan** – Restore affected systems to normal business operation.
- **Incident Learning** – What can be learned from this incident? What can be improved so this type of incident does not again?

## What about regular surveillance?

Many companies overlook the fact that security monitoring or surveillance is necessary in order to protect their information assets. Security Information Management Systems (SIM), if configured properly, can be useful in collecting and correlating security data



(system logs, firewall logs, anti-virus logs, user profiles, physical access logs, etc.) to help identify internal threats and external threats. A successful surveillance program includes practices such as:

- Security in Depth is a best practice. Several layers of security are better than one. Surveillance on each layer of security will help identify the severity of a security event; alerts coming from the internal corporate network might be more urgent than on the external network.
- Critical business data should be encrypted with strict role-based access controls and logging of all changes for an accurate audit trail.
- A policy of “least privileges access” should always be implemented with respect to sensitive information and logs should be reviewed regularly for suspicious activity.
- Review of Identity Management Process to determine who has access to what information on the corporate network. Ensure that the access of ex-employees, contractors and vendors is eliminated when they are no longer needed or leave the organization.
- Placement of Network Intrusion Detection/Prevention Systems throughout the corporate network to help detect suspicious or malicious activity.

## What about access controls?

Curiosity is a natural human trait. The viewing of private records of political figures and celebrities has led to people losing their jobs or being criminally convicted. Most of these workplace incidents were not tied to identity theft or other bad intentions, but were simply instances of employees taking advantage of access control policy gaps, sometimes without realizing that they were breaking privacy laws and exposing their organizations to risk.

So companies need to focus on ensuring that employees’ access to information is required for their particular job. Sometimes employees’ access is supplemented as they are promoted, transferred, or temporarily assigned to another department within the organization. Users that drag such excess access into their new role may create holes in corporate security or create other business risks. These are common problems in large organizations, a natural consequence of the pressure on IT departments to provide access quickly when employees are transferred or promoted.

Organizations should consider putting automated controls in place for cyber-access to ensure that user privileges are appropriate to their particular job function or process role. Access to personally identifiable information must be governed by the need; there must be a valid business reason for access.

## Security Training and Awareness

The human factor is the weakest link in any information security program. Communicating the importance of information security and promoting safe computing are key in securing a company against cyber crime. Below are a few best practices:

- Use a “passphrase” that is easy to remember — E@tUrVegg1e\$ (Eat your veggies) and make sure to use a combination of upper and lower case letters, numbers, and symbols to make it less susceptible to brute force attacks. Try not to use simple dictionary words as they are subject to dictionary attacks – a type of brute force attack.
- Do not share or write down any “passphrases.”
- Communicate/educate your employees and executives on the latest cyber security threats and what they can do to help protect critical information assets.
- Do not click on links or attachments in e-mail from untrusted sources.
- Do not send sensitive business files to personal email addresses.
- Have suspicious/malicious activity reported to security personnel immediately.
- Secure all mobile devices when traveling, and report lost or stolen items to the technical support for remote kill/deactivation.
- Educate employees about phishing attacks and how to report fraudulent activity.

## Conclusion

The risks of cyber crime are very real and too ominous to be ignored. Every franchisor and licensor, indeed every business owner, has to face up to their vulnerability and do something about it. At the very least, every company must conduct a professional analysis of their cyber security and cyber risk; engage in a prophylactic plan to minimize the liability; insure against losses to the greatest extent possible; and implement and promote a well-thought-out cyber policy, including crisis management in the event of a worst case scenario.

## Appendix of links to articles on cyber crime

How to Jailbreak 1.1.1 only ipodtouch or iphone (script kiddie example )

<http://www.youtube.com/watch?v=keO9K0kgJI&feature=related>

RSA Conference 2007: FTC planning new methods to combat ID theft (FTC chairman was a victim)

<http://www.scmagazine.com/asia/news/article/632058/rsa-conference-2007-ftc-planning-new-methods-combat-id-theft/>

TJX settles with MasterCard for \$24 million

<http://www.scmagazineus.com/TJX-settles-with-MasterCard-for-24-million/article/108671/>

FTC settles breach case with Reed Elsevier and Seisint (TJX data brokers)

<http://www.scmagazineus.com/FTC-settles-breach-case-with-Reed-Elsevier-and-Seisint/article/108400/>

Hannaford tells regulators how breach happened

<http://www.scmagazineus.com/Hannaford-tells-regulators-how-breach-happened/article/108569/>

Horizon 300,000 members unencrypted data on stolen laptop

<http://www.scmagazineus.com/Horizon-300000-members-unencrypted-data-on-stolen-laptop/article/104737/>

ChoicePoint settles lawsuit over 2005 breach

<http://www.scmagazineus.com/ChoicePoint-settles-lawsuit-over-2005-breach/article/104649/>

Data of 650,000 customers of JCPenney, retailers at risk

<http://www.scmagazineus.com/Data-of-650000-customers-of-JCPenney-retailers-at-risk/article/104368/>

Discount retail website Geeks.com hacked

<http://www.scmagazineus.com/Discount-retail-website-Geekscom-hacked/article/100508/>

Florida woman accused of deleting \$2.5 million in data (Insider Threat)

<http://www.scmagazineus.com/Florida-woman-accused-of-deleting-25-million-in-data/article/104575/>

Analysts: French bank could have stopped \$7 billion insider fraud

<http://www.scmagazineus.com/Analysts-French-bank-could-have-stopped-7-billion-insider-fraud/article/104586/>

Interesting Metrics from IC3 (Internet Crime Consortium), FTC, and idtheftcenter.

<http://www.scmagazineus.com/2008-on-pace-for-record-number-of-breaches/article/108685/>

IC3 report: Internet crime up to \$240 million in 2007

<http://www.scmagazineus.com/IC3-report-Internet-crime-up-to-240-million-in-2007/article/108706/>

2008 Breach List

[http://www.idtheftcenter.org/artman2/publish/lib\\_survey/ITRC\\_2008\\_Breach\\_List.shtml](http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml)

Thieves Winning Online War, Maybe Even in Your Computer - 12/6/08

[http://www.nytimes.com/2008/12/06/technology/internet/06security.html?\\_r=1&hp](http://www.nytimes.com/2008/12/06/technology/internet/06security.html?_r=1&hp)

One Hacker's Audacious Plan to Rule the Black Market in Stolen Credit Cards

[http://www.wired.com/techbiz/people/magazine/17-01/ff\\_max\\_butler](http://www.wired.com/techbiz/people/magazine/17-01/ff_max_butler)

Tech security: Most big companies unprepared for IT risks, survey finds

<http://www.finance-commerce.com/article.cfm/2009/01/06/Tech-security-Most-big-companies-unprepared-for-IT-risks-survey-finds>

Data Breaches Up Almost 50 Percent, Affecting Records of 35.7 Million People

<http://www.washingtonpost.com/wp-dyn/content/article/2009/01/05/AR2009010503046.html?hpid=moreheadlines>

FTC May require new Identity Theft Programs

<http://www.franchise.org/Franchise-News-Detail.aspx?id=43488#two>

ANSI Launches Guide to Help Calculate Cyber Security Risk

<http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=211600785>

Blaine man pleads guilty to placing virus in computers

[http://www.startribune.com/local/north/37542054.html?elr=KArksD:aDyaEP:kD:aUbP:P:Q\\_V\\_MPQLa7PYDUiD3aPc:\\_Yyc:aUU](http://www.startribune.com/local/north/37542054.html?elr=KArksD:aDyaEP:kD:aUbP:P:Q_V_MPQLa7PYDUiD3aPc:_Yyc:aUU)

Windows worm numbers 'skyrocket'

<http://news.bbc.co.uk/2/hi/technology/7832652.stm>

Clock ticking on worm attack code

<http://news.bbc.co.uk/2/hi/technology/7832652.stm>

Card Data Breached, Firm Says (same as below)

<http://online.wsj.com/article/SB123249174099899837.html?mod=testMod>

Firm Reports Massive Data Breach From Credit, Debit Transactions (same as above)

<http://www.washingtonpost.com/wp-dyn/content/article/2009/01/20/AR2009012003674.html?hpid=news-col-blog>

Frequency and Severity of Data Breaches Have Led to Changes in How Companies Are Underwriting the Risk

<https://plusweb.org/index.cfm/p/Journal.Article/articleID/100061.htm>

Worm Infects Millions of Computers Worldwide  
<http://www.nytimes.com/2009/01/23/technology/internet/23worm.html?hp>

Scammers Replace Credit Card Readers in Irish Stores  
[http://www.pcworld.com/businesscenter/article/149935/scammers\\_replace\\_credit\\_card\\_readers\\_in\\_irish\\_stores.html](http://www.pcworld.com/businesscenter/article/149935/scammers_replace_credit_card_readers_in_irish_stores.html)

Job website hit by major breach  
<http://news.bbc.co.uk/go/rss/-/1/hi/technology/7853251.stm>

Feds Ready to Tackle Cybercrime  
[http://www.abajournal.com/magazine/feds\\_ready\\_to\\_tackle\\_cybercrime](http://www.abajournal.com/magazine/feds_ready_to_tackle_cybercrime)

Businesses risk \$1 trillion losses from data theft: study  
[http://mobile.reuters.com/mobile/m/FullArticle/p.rdt/CTECH/notechnologyNews\\_uUSTRE50S2FX20090129](http://mobile.reuters.com/mobile/m/FullArticle/p.rdt/CTECH/notechnologyNews_uUSTRE50S2FX20090129)

Cybercrime threat rising sharply  
<http://news.bbc.co.uk/2/hi/business/davos/7862549.stm>

Suit Alleges Internet Espionage  
<http://online.wsj.com/article/SB123353995726038063.html?mod=testMod>

Data breach costs, customer churn up a bit; Repeat offenders abound  
<http://blogs.zdnet.com/BTL/?p=12015&tag=nl.rSINGLE>

FBI Uncovers Worldwide \$9M ATM Card Scam  
<http://www.foxnews.com/story/0,2933,487184,00.html>

Parking ticket leads to a virus  
<http://news.bbc.co.uk/2/hi/technology/7872299.stm>

Obama begins cybersecurity review  
<http://news.bbc.co.uk/2/hi/technology/7880695.stm>

Judge OKs \$20 Million Payment in Data Theft Case  
<http://www.nytimes.com/aponline/2009/02/10/washington/AP-Vets-Data-Theft.html>

Crooks set cyber traps on Digg: security firm  
[http://rawstory.com/news/2008/Crooks\\_set\\_cyber\\_traps\\_on\\_Digg\\_0211.html](http://rawstory.com/news/2008/Crooks_set_cyber_traps_on_Digg_0211.html)

Malicious insider attacks to rise  
<http://news.bbc.co.uk/2/hi/technology/7875904.stm>

Hackers warn high street chains  
<http://news.bbc.co.uk/2/hi/technology/7366995.stm>

Microsoft bounty for worm creator

<http://news.bbc.co.uk/2/hi/technology/7887577.stm>

Do We Need a New Internet?

<http://www.nytimes.com/2009/02/15/weekinreview/15markoff.html?ref=weekinreview>

Researchers Hack Faces In Biometric Facial Authentication Systems

<http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml;jsessionid=1TT4XOGIH D2DCQSNDLRSKHSCJUNN2JVN?articleID=213901113>

Personal Data Of 45,000 Exposed In FAA Data Breach

<http://www.darkreading.com/security/attacks/showArticle.jhtml?articleID=213402894&cid=RSSfeed>

CVS to pay \$2.25 million to settle HIPAA violation

<http://www.scmagazineus.com/CVS-to-pay-225-million-to-settle-HIPAA-violation/article/127570/>

## Appendix - Glossary of Cyber Security Terms

### *How Computers Work*

- **Hardware** – All of a computer’s physical components including the mouse, keyboard, screen, and printer as well as internal parts like the processor and hard drive.
- **Operating system** – Creates the connection between the computer’s hardware and the application software employed by the user. Common operating systems include Microsoft Windows, MacOS and Linux.
- **Software** – A set of instructions that cause the computer to perform certain tasks; can be divided into two types: system software and application software
- **Browsers** – Programs that look through content published on the Internet and display Internet pages. The most commonly used browsers are Microsoft Explorer and Mozilla Firefox.

### *Vulnerabilities*

- **Malware** – The name given to malicious software that operates under the guise of a useful software program. It runs computer processes that are either unexpected or unauthorized but always harmful. The term “malware” generally covers viruses, worms and Trojans.
- **Viruses** – Software with the ability to self-replicate and attach itself to other executable programs. The behavior is comparable to its biological counterpart. Computer viruses can also be contagious (might spread on or even beyond the infected computer), exhibit symptoms (the presence of malicious code and its magnitude) and involve a recovery period with possible long-term effects (difficulty in removal and loss of data).
- **Worm** – An autonomous program or constellation of programs that distributes fully functional whole or parts of itself to other computers. Worms are specialists in spreading and reproducing. They consistently exploit all known vulnerabilities, including people, to penetrate barriers that seem to be impenetrable to normal viruses. A worm does not have a payload of its own but is often used as a transport mechanism for viruses that ride piggyback and immediately start their work.
- **Grayware** – Applications that cause annoying behavior in the way programs run. Unlike malware, grayware does not fall into the category of major threats. Grayware is not detrimental to basic system operations.
- **Spyware** – Software that installed under misleading premises that monitors and collects a user’s data and eventually transmits it to a company for various purposes. This typically happens in the background - that is, the activity is invisible to most users.
- **Phishing** – A method of stealing personal data whereby an authentic-looking e-mail is made to appear as if it is coming from a real company or institution. The idea is to trick the recipient into sending secret information such as account information or login data to the scammer.

- **Dialers** – Dialing programs used to dial up an Internet connection using preset and typically overpriced phone numbers.
- **Backdoor** – An application or service that permits remote access to an infected computer. It opens up a so-called backdoor to circumvent other security mechanisms
- **Adware** – Software that displays banner ads or pop-ups when a computer is in use. The presence of adware is likely if dubious offers are displayed as pop-ups or banner ads even when you are visiting a reputable website and have a pop-up blocker enabled. Even though adware is not classified as harmful malware, many users regard it as irritating and intrusive. Adware can often have undesired effects on a system, even interrupting the Internet connection or system operations.
- **Trojans** – From Greek legend of the Trojan Horse. In the world of computers, it refers to covert infiltration by malicious software under the guise of a useful program. After a Trojan is activated, it is often very difficult to discover the extent of the damage and generally identify the malware. The Trojan may change its original name and reactivate every time a PC is started.

### *Protection*

- **Anti-virus software** – Software that detects and removes viruses.
- **Firewalls** – A personal firewall is a program that works on a PC as a protective filter for data communication in a potentially dangerous network such as the Internet.



## About the Authors

**Bruce S. Schaeffer**, co-author of *CCH Franchise Regulations and Damages* and author of the BNA Tax Management Portfolio on Franchising, is an attorney in private practice with over 30 years' experience and offices in New York City. Mr. Schaeffer holds a Master of Laws (in Taxation) from New York University School of Law and a Juris Doctor degree from Brooklyn Law School. He has spoken before audiences at the New York University Institute on Federal Taxation, the Practising Law Institute, the International Franchise Association, the New York State Bar Association, and many other forums. Mr. Schaeffer is the founder and president of Franchise Valuations, Ltd. ([www.franchisevaluations.com](http://www.franchisevaluations.com)), which provides expert testimony on damages and valuations in franchise disputes, performs lender due diligence, and resolves succession and estate planning problems for the franchise community. He is a member of the Institute of Business Appraisers, the American Association of Franchisees and Dealers, the American Bar Association, and the New York State Bar Association. Mr. Schaeffer has been named a "Legal Eagle" by *Franchise Times* magazine.

**Henfree Chan**, a co-founder of Franchise Technology Risk Management, is a Senior Information Security Professional with 10 years' experience in the financial services industry. He has worked at the world's most prominent financial institutions, including Goldman Sachs and Deutsche Bank, helping them to develop, implement, and enforce strategic global security monitoring, data protection, and incident response programs to support regulatory compliance (Basel II, Gramm-Leach-Bliley, Sarbanes-Oxley, and PCI DSS) in the banking industry. His specialties include penetration testing, threat and vulnerability management, incident response, malicious code analysis, and security architecture. Henfree holds a Bachelor of Science degree in Engineering Management Systems from Columbia University's School of Engineering and Applied Science.

**Henry Chan**, a co-founder of Franchise Technology Risk Management, is also founder and president of H2 IT Management, Inc., a New York City network consulting firm that specializes in end-to-end Internet and technology solutions. Previously he was a market maker for Spear, Leeds and Kellogg, the largest specialist trading firm on the NYSE and NASDAQ/AMEX. Before that, as a project manager for IKON Office Solutions, he managed "paperless office solutions" projects for the general counsel's office of the American International Group, for Phelps Dodge Corporation, and for the law firms of Oblon Spivak and Dewey Ballantine. Before joining IKON, he was assistant operations supervisor at Net Matrix, a full-service imaging consulting firm specializing in UNIX-based operating platforms. At Net Matrix he supervised facilities management projects and provided consulting and training services for investment banking and law firm clients. Henry earned a Bachelor of Business Administration in finance from Baruch College of The City University of New York.

**Susan Ogulnick** is Vice President of Research and Operations for Franchise Valuations, Ltd. She has more than 20 years of experience in the information industry and is a recognized authority in acquiring information about hard-to-value entities. Ms. Ogulnick earned a Masters of Business Administration degree from New York University. She also holds M. Phil. and M.A. degrees in Political Science from Columbia University. Ms. Ogulnick was formerly Vice President of Consulting Services at FIND/SVP, Inc., a worldwide business advisory and research service.