Emerging Issues For E-Commerce Businesses:

Updates and Developments in 2015

The Knowledge Group
Webcast Series

Neff
LAW FIRM
a professional law corp.

Richard Neff
richard@nefflaw.com
310.321.7660

1600 Rosecrans Ave.
Media Center-4th Floor
Manhattan Beach, CA 90266

November 00, 2014

B2B Legal Issues

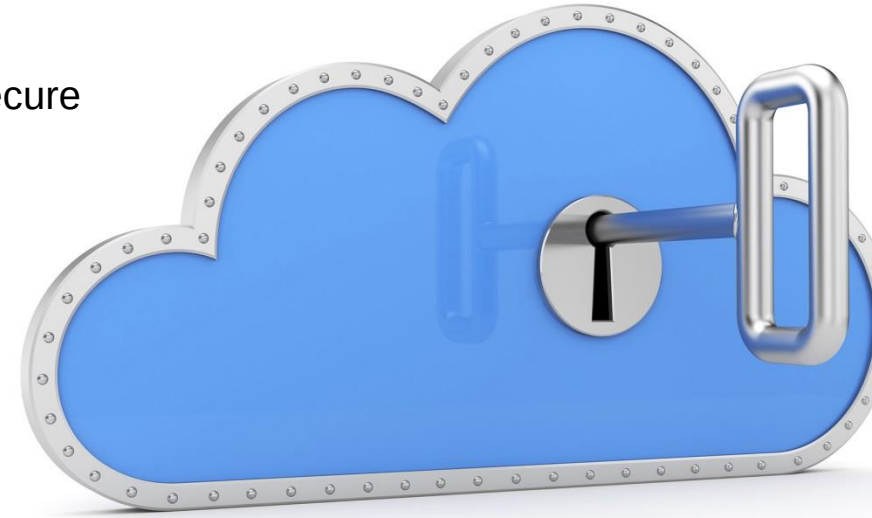
- B2B is focused on supply chain management
- Portals allow businesses to deal directly with suppliers and distributors online
- Electronic orders, invoicing, payment, Cloud hosting of IT
- B2C links customers to suppliers or social networks, e.g., Amazon, eBay, Facebook, Craigslist

Biggest Concern: Cyber-Security & Data Breaches

- Every day the sensitive personal information of millions of Americans is stolen
- A who's who of companies have not proved secure enough:

  Target, Home Depot, USPS
- The Cloud is efficient and scalable, but also hard to secure
- Hackers target US innovation, seeking commercial

  advantage, esp. from Russia and China



How Can a Business Ensure its Security?

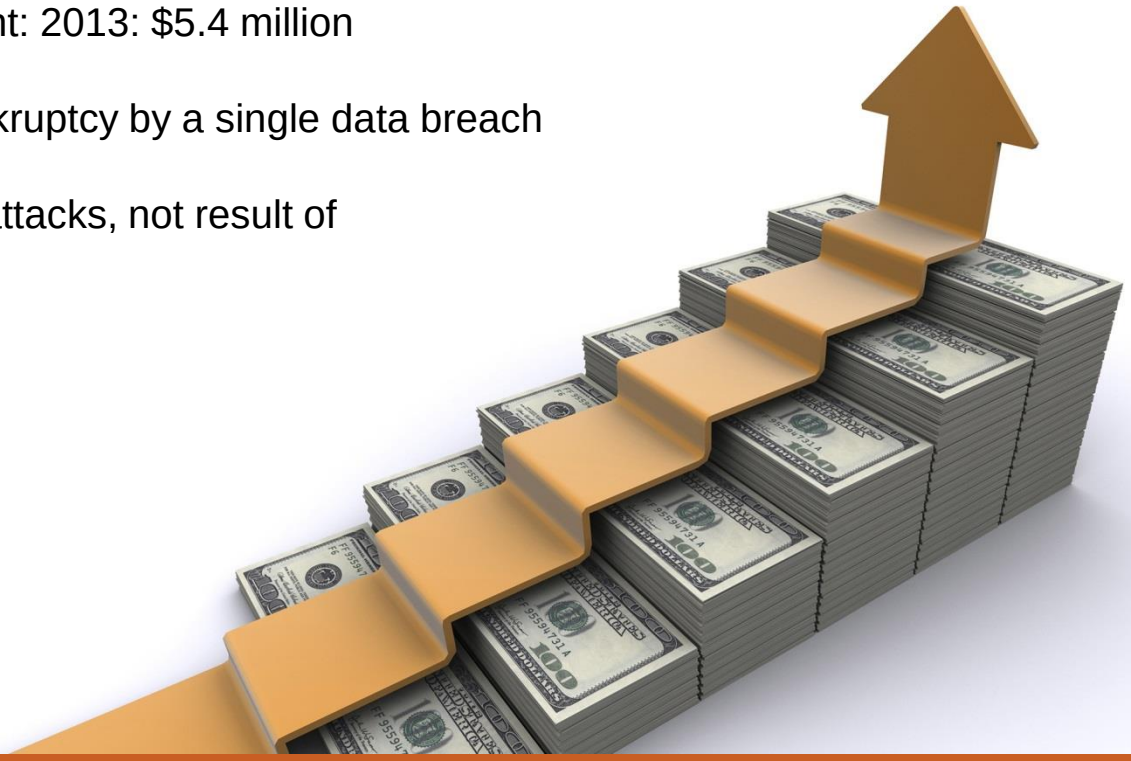
- Over time nothing is hack-proof
- But IT departments need to ensure that a business (as provider or consumer) is secure
- Ecommerce sites need sophisticated object-oriented programming languages, internal networks removed from public-facing servers, and secondary dynamic authentication
- Use strong SSL authentication for web and data protection; look for SSL security seal
- If taking credit cards, be PCI compliant
- Try not to store sensitive data, especially credit card information
- Require strong passwords
- Set up system alerts for suspicious activities
- Layer your security, firewalls, login boxes, search queries
- Train your employees (laptop problem)

Evolving Standards for Cybersecurity

- Certify to ISO 27001 family of standards, best practices for keeping information assets secure
- Commerce Department's National Institute of Standards & Technology (NIST) released in February "Framework for Improving Critical Infrastructure Cybersecurity"
- Provides a structure that organizations, regulators and customers can use to create, guide, assess or improve cybersecurity programs
- Intended for organizations regardless of size to apply best practices of risk management to cybersecurity

Cost to Businesses with Sites that Suffer Data Breach

- The leading problem is the crushing cost: average per capita cost of data breach in 2013: $188
- Average number of breached records in any incident: 2013: 28,765 [Symantec data]
- Organizational average cost per incident: 2013: $5.4 million
- Small businesses often forced into bankruptcy by a single data breach
- Most attacks are malicious or criminal attacks, not result of negligence or system glitches



Legal Response to Data Breach

- US does not have required corporate standards except in certain sectors (financial services/health records-HIPAA)
- My client, music technology manufacturer, had part of its customer database hacked, with est. 1000 personal records stolen and published on a website in Asia
- First, careful research is required, to determine exactly what data was stolen, and from whom
- I had the website taken down by contacting the Asian webhost, mitigating harm
- Made sure my client complied fully with California's data breach notification law

State Laws on Security Breach Notification Law

- Only 3 states lack such law (Alabama, New Mexico, South Dakota)
- California has new law governing security breach notification since 2012, copied by many states
- Requires any company doing business in CA to notify CA residents whose ***unencrypted*** Personal Information was/believed to be acquired by unauthorized person through security breach
- Law prescribes (a) when notice must be sent, (b) what form notice must take (physical notice or email), and what the notice must contain
- Incident must be described, timing of incident disclosed, and contact information given for the business
- Type of personal information hacked must be disclosed, and if the breach exposes SS Number or driver's license number, toll free numbers of major credit reporting agents must be provided
- If breach affects 500 or more California residents, state attorney general must be notified
- Takeaway: encrypting personal information is wise

Personal Data Privacy: US and abroad

- Personal data privacy is a related issue, governed by legislation in most of the world
- The US is an outlier, without comprehensive federal regulation except for certain sectors
- The Graham-Leach-Bliley Act regulates financial information, and HIPAA regulates medical information
- FTC takes action against unfair/deceptive privacy and data security policies, and enforces the Children's Online Privacy Protection Act (regulating collection of information from children under 13)
- State laws: California was the first to enact a stringent privacy law (2003), and the strictest are in Massachusetts, New York and Virginia, all tending toward European laws
- But much of the world has followed very stringent EU model, carefully regulating treatment of personally identifiable information (and sensitive personal information) about individuals
- This makes US E-Commerce entrepreneurs more cavalier about personal data privacy than their European counterparts, leading to frequent violation of other countries' laws

European Privacy Protection – Evolving International Standard

- All EU members have enacted laws that reflect the EU Directive on Data Protection
- Covers “personal information”-information that can be used to identify a natural person, directly or indirectly
- Applies to all processing of data, online or not, automatic or manual, excluding only “purely personal or household activity”
- Establishes requirements for notice, consent of data subject, accuracy, security and access
- Stricter for “sensitive data”, e.g., pertaining to racial or ethnic origins, political or religious beliefs, or health or sexual activity or preference (explicit consent of data subject required)
- Each member state must establish governmental authority to oversee
- Member states must enact laws prohibiting transfer of data to countries outside of EU that fail to ensure “adequate level of protection”—aimed at US

US Companies and Data Transfer Abroad

- Online US businesses, or multinationals, or any business that moves personal information from Europe to US servers (or elsewhere) is likely to violate European law
- European privacy laws generally mandate tough sanctions and penalties
- Canada also has extremely tough privacy laws (plus overlay of provincial laws)
- Therefore, companies need express consent from data subjects to transfer personal data, which can be unrealistic re: batch transfers
- US companies can overcome this problem by subscribing to US Department of Commerce's Safe Harbor Framework Principles
- It is voluntary self-certification process, relatively easy to achieve, requires annual filing and small payment
- Agreement between US and EU+Switzerland permits transfers to companies which are Safe Harbor compliant

The FTC and Data Security/Privacy

- Since 2000, FTC has brought more than 40 data security enforcement actions
- FTC in 2011 reached consent order with Facebook, ending long investigation into Facebook user privacy practices
- Facebook agreed not to misrepresent extent to which it maintains privacy or security of user provided information, must clearly indicate what user information is nonpublic, and is subject to privacy audits every 2 years for 20 years
- Twitter and Google also subject to FTC consent orders
- In 2014, FTC has negotiated settlements with Fandango and CreditKarma for alleged failures to take reasonable steps to secure consumers' personal information
- FTC relies on Section 5(a) of the FTC Act: "unfair or deceptive acts or practices in or affecting commerce…are…declared unlawful."
- Unfair practices tend to be those that cause or are likely to cause substantial injury to consumers, not reasonably avoidable by consumers, and not outweighed by benefits
- Make sure your company complies 100% with its privacy policy: not enough to copy one by another company that you respect
- Confirm that your data security practices are up to industry standards, especially encryption of personal information

The FTC and Online Contracts Generally

- FTC has taken action against other online contracts which it believed to be unfair or deceptive to consumers under FTC Act
- In 2009 FTC filed complaint against Sears alleging that it did not adequately disclose the actual function of the software tracking application that it offered
- Earlier this year FTC settled with 12 US businesses charged with falsely claiming they were abiding by the US-EU Safe Harbor Framework Principles, including Atlanta Falcons, Level 3 Communications, Reynolds Consumer Products, BitTorrent
- While FTC privacy and data security enforcement is a key focus, companies need to ensure that they also fully comply with their online Terms of Service or Use (deceptive or unfair practices)

Key Threat to E-Commerce: Cyber Fraud

- Credit Card Fraud is rampant on the Internet, with frequent phishing and attempts to obtain credit card information, often in scams perpetrated by false Internet marketing and retail enterprises
- Internet auction fraud and failure to deliver merchandise purchased online is common
- Internet Investment Fraud is common
- Companies suffer from sales of counterfeit goods on copycat websites that mirror legitimate sites (often Russian mafia or other crime syndicates)

Click Fraud: Ongoing Problem in B2B E-Commerce

- Click fraud: generating ad impressions either using non-human sources, e.g., lines of code or bots that click on a brand's ads, or hiring lots of users to manually click on the same ad.
- Classic click fraud is illegal manipulation of keyword-based advertising: one company can click on a rival's search engine ads to drive up its costs, or use spyware to force views or clicks, forcing the target to pay the search engine for each click
- A variation targets ads fed to websites, from personal blogs to major corporate websites, by search providers like Google (AdSense), Yahoo!, MSN: if a blog visitor clicks on the ad, the search engine splits its fee with the blogger
- Some claim in 2014 that up to 50% of all clicks on billed-for ads are generated by non-human traffic
- In 2014, Interactive Advertising Bureau estimated that in 2014, click fraud will cost marketers $11.6 billion in advertising, up 22% from 2013, according to survey findings
- Last year Google said it disabled 2 million bad ads, banned 14,000 advertisers for selling counterfeit goods, disabled more than 5,000 AdSense accounts

Internet Taxation and E-Commerce

- Online only retailers in the US have had advantage over brick-and-mortar retailers
- The latter collect and pay sales taxes in all cases
- More than 25 states have enacted legislation on this subject, making it easier for out of state sellers to collect and remit sales tax
- Some states have enacted affiliate nexus or “Amazon” laws, some have increased reporting requirements by retailers
- Amazon now collects tax in 21 states, including California
- US Senate in 2013 approved Marketplace Fairness Act where states that meet certain requirements can require out-of-state retailers that have more than $1 million in out-of-state sales to collect and remit state sales tax, stuck in House of Representatives

Neff
LAW FIRM
a professional law corp.

Richard Neff
richard@nefflaw.com
310.321.7660

1600 Rosecrans Ave.
Media Center-4th Floor
Manhattan Beach, CA 90266

November 00, 2014