



Privacy And Data Protection - Common Sense Solutions To New Threats

Joe Ortego

Nixon Peabody (New York, NY)

jortego@nixonpeabody.com | 212.940.3045

http://www.nixonpeabody.com/joseph_j_ortego

PRIVACY AND DATA PROTECTION



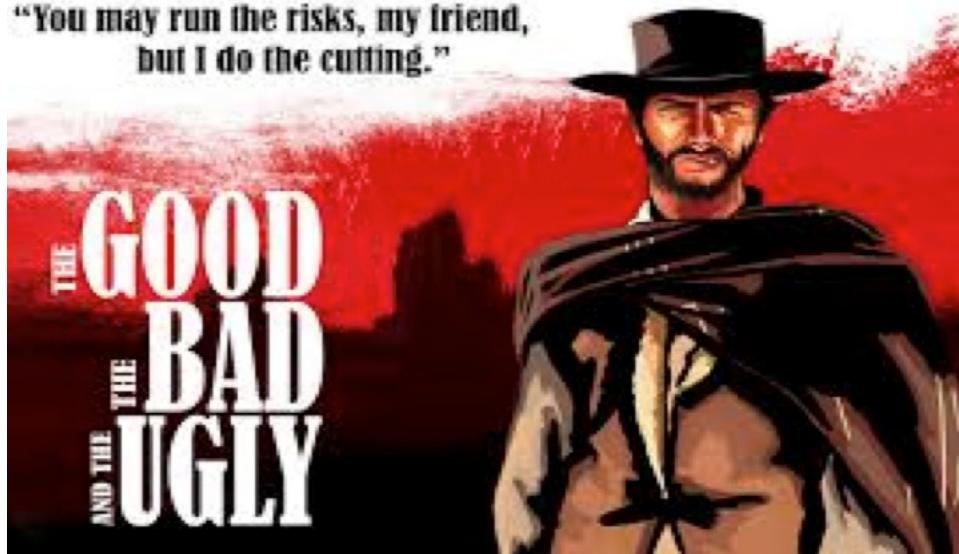
BY: JOSEPH ORTEGO
437 MADISON AVENUE
NEW YORK, NY 10022-7039
PHONE: (212) 940-3000

HOW DO YOU PROTECT YOUR COMPANY?



DATA

"You may run the risks, my friend,
but I do the cutting."

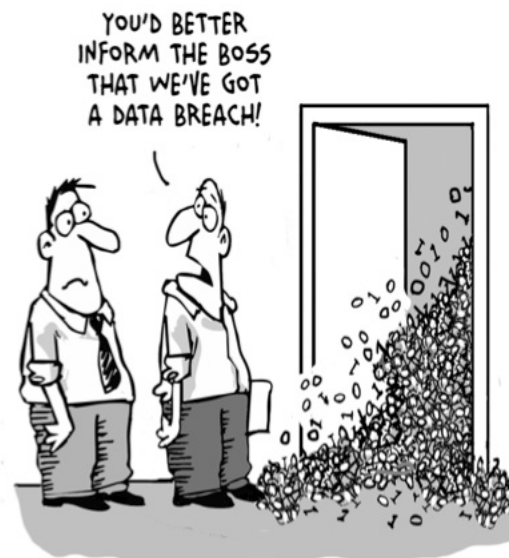


WHAT IS A DATA BREACH?



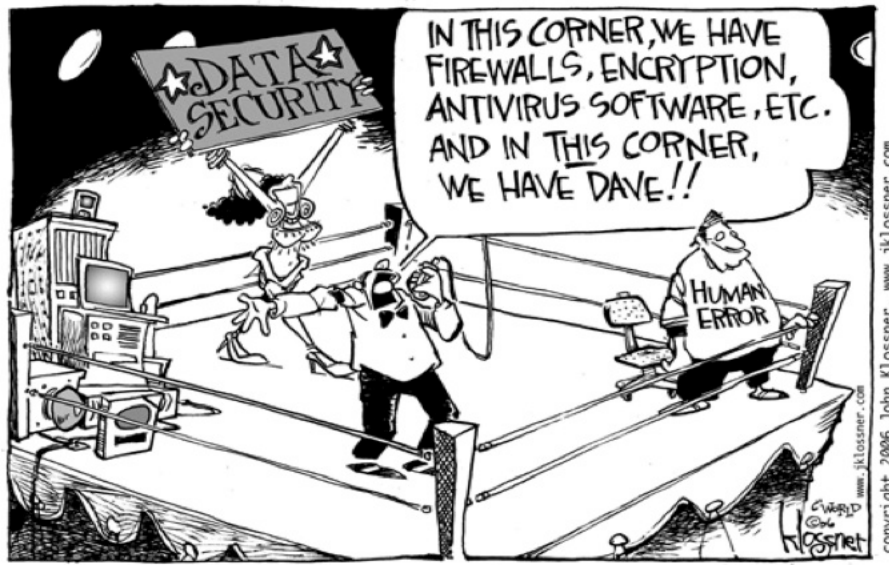
REACTIONS

~ Knowing how to react after a breach will make a difference to your company's image and what it will cost you.



© D.Fletcher for CloudTweaks.com

STEPS AFTER A BREACH



VALUE OF OUTSIDE COUNSEL

ATTORNEY CLIENT PRIVILEGE

In house counsel wears many different hats- question of what communications between whom are protected. Specifically between in-house counsel and members of the corporation.

WORK PRODUCT

When outside counsel is called in it is clear that the documents they put together fall under the work product rule and are not created for business purposes outside the suit.

NEW YORK NOTIFICATION REQUIREMENTS



FTC RED FLAG

TIP SHEET

PLAYING IT SAFE

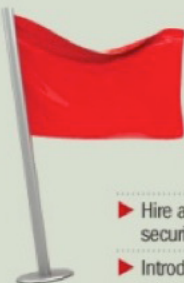
Tips in developing a Red Flags Rule program that enforces, detects, prevents and mitigates identity theft include:

To develop security policies and training:

- ▶ Implement and train employees to follow formal information security policies that protect the private information of employees and customers.
- ▶ Limit the number of people who have access to and/or handle confidential documents.
- ▶ Be careful when hiring new employees and perform full reference checks. Where warranted, ask new hires to sign confidentiality agreements.
- ▶ Demonstrate a commitment to the total security of your business and customer information.

To implement an information security strategy:

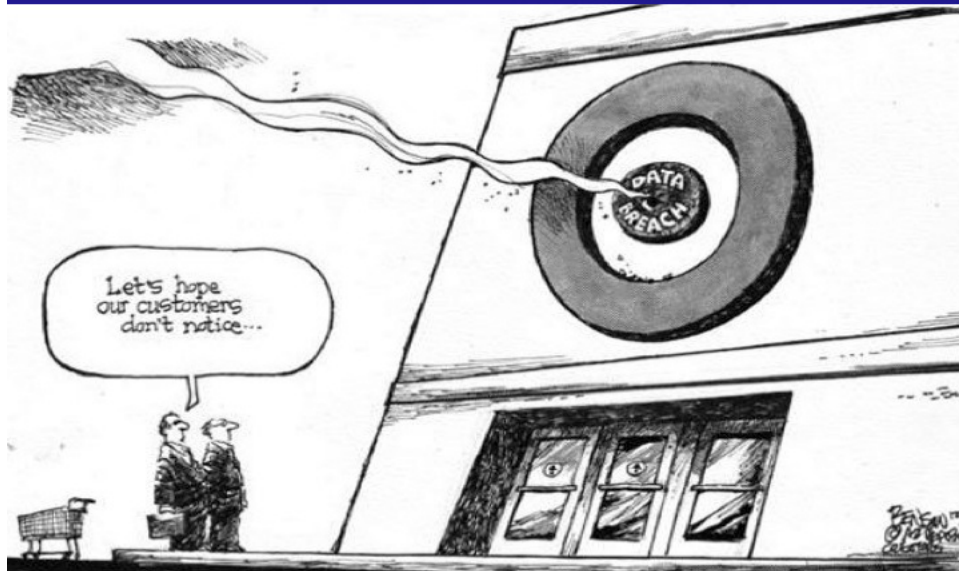
- ▶ Conduct a periodic security audit to confirm that policies are being upheld.
- ▶ Identify and seal security loopholes at every stage of the information cycle, from data generation and storage to the transfer of data from location to location and document destruction.
- ▶ Develop a comprehensive strategy to manage unique security risks. Target both paper-based and electronic information sources.
- ▶ Hire a reliable security vendor to address all information security needs to prevent security breaches and fraud.
- ▶ Introduce a "shred-all" policy, to ensure that all waste paper is securely destroyed on a regular basis.



FEDERAL TRADE COMMISSION



BREACHES



WHAT CAN YOU DO?

STAR TRIBUNE
BOOK



1. Awareness is your best defense!
2. Polices are important
3. You get what you pay for
4. Security in not just technology-
it involves the people you hire as well
5. Compliance.....who is accountable
6. Ask questions!



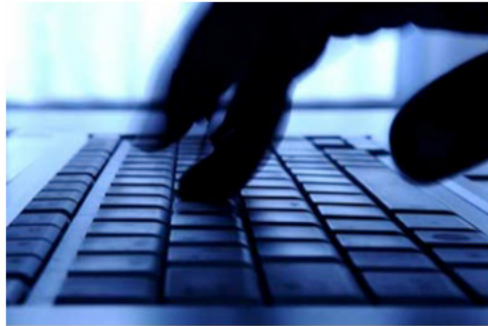
Rise in Cybercrime

- In less than 15 years, cybercrime has moved from obscurity to the spotlight of consumers, the corporate world, and national security.



Rise in Cybercrime

- As the world goes mobile, cybercrime will follow.



Cybercriminals are

- Financially motivated
- Increasingly sophisticated



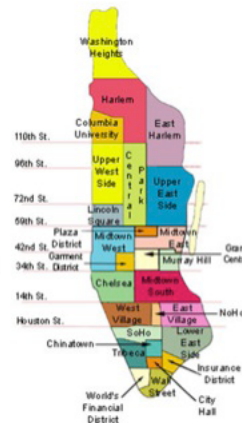
The Impact of Cybercrime

- Disrupts critical operations, exposes sensitive personal and business information, and it imposes high costs
 - The cost of investigating and responding to an attack
 - Expenses relating to customer support and public relations
 - Potentially even financial penalties and lawsuits



Cybercrime and the Manhattan District Attorney's Office

- Handles approximately 100,000 criminal cases per year
- 37% of all felony complaints drafted involve cybercrime or identity theft charges
- District Attorney Vance created the Cybercrime and Identity Theft Bureau in 2010



New York State White Collar Crime Task Force

- District Attorney Vance has sought, via his leadership of the White Collar Crime Task Force, to amend existing New York State law



New York State White Collar Crime Task Force

Recommendations on Cybercrime and Identity Theft:

1. Expand the definition of “computer material”
2. Upgrade Computer Tampering and create a first-degree crime
3. Gradate the existing crime of Identity Theft

Expand the Definition of “Computer Material”

- “Computer material” is restricted to medical records, government records, or data that provides a competitive advantage to the individual accessing it without permission.
- Broaden the definition of “computer material” to allow both Computer Trespass and Computer Material to be treated with the seriousness they deserve in non-commercial situations

Upgrade Computer Tampering and Create a First-Degree Crime

- Computer Tampering is currently capped at a Class C felony
- Upgrade Computer Tampering and create a new Class B felony for Computer Tampering that causes a loss of \$1 million or more

Graduate the Existing Crime of Identity Theft

- Graduate Identity Theft to create crimes ranging from a Class A misdemeanor to a Class B felony, based on dollar threshold amounts *or* the number of identities assumed
- A defendant who buys one handbag at \$2,001 using one stolen credit card faces the same top count as a defendant who buy 1,000 handbags, each at \$2,001, using 1,000 stolen credit cards

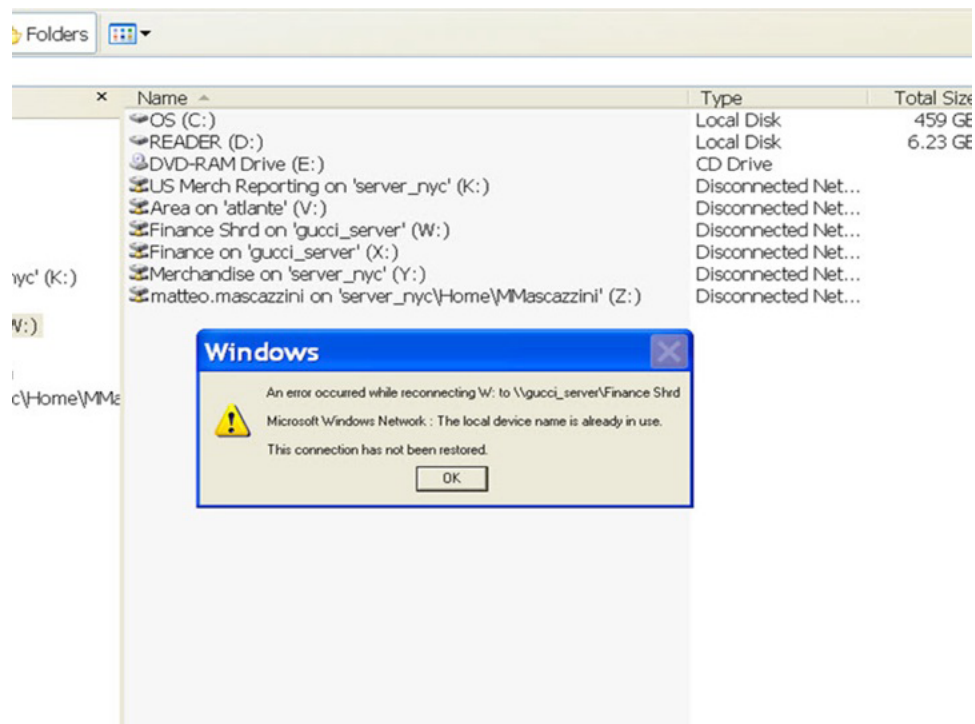
The Threat Landscape

1. Hacking of Computer Networks, Systems, and Databases
2. Theft of Personal Identifying Information
3. Intellectual Property Theft



Gucci Network Attack

- In November 2010, the corporate computer network of Gucci America, Inc. was attacked
- Total disruption of business operations, corporate e-mail mailboxes were deleted and pre-holiday season annual inventory data inaccessible
- Three servers on the network were found to have been compromised



Gucci Network Attack

- One Gucci reserved IP address, 10.80.29.98, was found to have accessed all 3 servers prior to the attack
- The intruder gained access through a VPN, which requires a physical token, submission of passwords and a username



Who was on the network using a VPN at the time?

	YSL Manager VIP Client Services	Norrell	TERM(40392)
	GGW Marketing Director	Marketing	Active
	GGW Senior Merchandiser East	Sales-East	Active
	Database Marketing Temp	Relational Marketing	TERM(1007001)
	YSL Operations & Loss Prevention Manager	Store Operations	Active
	GGW Independent Sales Manager	Independent Sales Region	Active
	Gucci MIS Store App Specialist	MIS	Active
	GGW Latin America Regional Director	Latin America	Active
	BV w/w Public Relations Event Production Manager	Public Relations World Wide	TERM(592078)
	GGW Regional Sales Manager	Sales- West	TERM(10092)
	Gucci Midrange System & Data Center Manager	MIS	Active
	Gucci w/w Manager of Entertainment Industry Relations	World Wide Public Relations	Active
	Gucci Junior PR Manager	Public Relations	TERM(1002078)
	GGW Regional Sales Manager- West	Independent Sales Region	Active
	YSL West Coast Regional Operations Manager	Non-Sell	Active
	Gucci Regional Sales Manager GGW Canada	GGW Canada	Active
	IBM Consultant	MIS	Active- but not a Gucci employee
"Bert"	"John"	None	None

< 164-Jun 12 2010 10:12:19 :%ASA-4-110019: Group = AMER-in, Username = John Bare, IP = 36.113.222.37, Session disconnected. Session Type: IPSecOverTCP, Duration: 0h:00m:41s, Bytes sent: 55357, Bytes rcvd: 31454, Reason: User Requested
 < 164-Jun 12 2010 17:38:49 :%ASA-4-110019: Group = AMER-in, Username = John Bare, IP = 36.113.222.37, Session disconnected. Session Type: IPSecOverTCP, Duration: 1h:24m:03s, Bytes sent: 482260781, Bytes rcvd: 2005643454, Reason: User Requested
 < 164-Jun 13 2010 21:32:14 :%ASA-4-110019: Group = AMER-in, Username = John Bare, IP = 36.113.222.37, Session disconnected. Session Type: IPSecOverTCP, Duration: 1h:53m:13s, Bytes sent: 36300266, Bytes rcvd: 9726452434, Reason: User Requested
 < 164-Jul Bytes sent: 0, Bytes rcvd: 0, Reason: User Requested
 < 164-Jul Bytes sent: 0, Bytes rcvd: 0, Reason: User Requested
 < 164-Jul Bytes sent: 0, Bytes rcvd: 0, Reason: User Requested
 < 164-Jul Bytes sent: 0, Bytes rcvd: 0, Reason: User Requested
 < 164-Jul Bytes sent: 0, Bytes rcvd: 0, Reason: User Requested
 < 164-Jun 30 2010 23:08:02 :%ASA-4-110019: Group = AMER-in, Username = John Bare, IP = 36.113.222.37, Session disconnected. Session Type: IPSecOverTCP, Duration: 1h:05m:12s, Bytes sent: 11167211, Bytes rcvd: 243203532, Reason: User Requested
 < 164-Jul 11 2010 20:47:39 :%ASA-4-110019: Group = AMER-in, Username = John Bare, IP = 36.113.222.37, Session disconnected. Session Type: IPSecOverTCP, Duration: 0h:00m:05s, Bytes sent: 7045, Bytes rcvd: 8031, Reason: User Requested
 < 164-Aug 05 2010 21:50:21 :%ASA-4-110019: Group = AMER-in, Username = John Bare, IP = 36.113.222.37, Session disconnected. Session Type: IPSecOverTCP, Duration: 0h:21m:03s, Bytes sent: 414629, Bytes rcvd: 1304367, Reason: Lost Service

<163> May 11 2010 00:14:47: %ASA-3-713119: Group = AMER-It, Username = Sam Yin, IP = 98.113.222.37, PHASE 1 COMPLETED

<164>May 11 2010 01:24:41 %ASA-4-113019: Group = AMER-int, Username = Sam Yin, IP = 98.113.222.37, Session disconnected. Session Type: IPSecOverTCP, Duration: 1h09m55s, Bytes xmt: 21961841, Bytes rcv: 121706940, Reason: User Requested

```
<64>Jun 12 2010 16:12:19: %ASA-4-113019: Group = AME7-int, Username = JohnBare, IP = 98.113.222.37, Session disconnected Session Type: IPSecOverTCP, Duration: 0h:00m:41s, Bytes xmt: 55357, Bytes rcv: 31454, Reason: User Requested
```

(164) Jun 12 2010 17:38:49: %ASA-4-110019: Group = AMER-int, Username = John Bare, IP = 98.113.222.37, Session disconnected. Session Type: PSecOverTCP, Duration: 1h:24m:09s, Bytes wmt: 482260781, Bytes rvt: 2005649454, Reason: User Requested

Who is Sam Yin?

- Former Gucci America network engineer
- Fired in May 2010 for abusing Gucci employee discount
- Had administrative access to all three systems attacked, intimately familiar with their operation
- VPN creation logs identify Sam Yin as the creator of the John Bare VPN token (prior to being fired)

How was the John Bare token activated?

Subject: Etoken locked up..
From: John Bare <john.baregucci@yahoo.com>
Date: Sat, 12 Jun 2010 11:41:29 -0700 (PDT)
To: support.services@us.gucci.com
X-RocketMail: 00000002;R--S-----;8089
X-YMail-OSG: DxhW0zYVM1IDUqVPkOH9CWhjWdJ3E_3QtuqrHo7JvY5V
fN3AMuYSBj85IFKUTI0gK0TR7RNjK6V1vLM8Bc_hdc4y8eu8Vd8ylUqfd5x
Ko61o06Gf_E.DL1tC6EAomahloDMERh4eKdMmJGEem2GysOpcYXuHr3KqUkK
KEOc_7FiHhRawSZDmdic0PEYaaC.sE4QxIW4RinHn_2WGgjiNaMgaUf35FM
R4ny1t5Nfmi70ri4bigAAg_nA1P7_EPLf
Received: from [98.113.222.37] by web114512.mail.gq1.yahoo.com via HTTP; Sat, 12 Jun 2010 11:41:29 PDT
X-Mailer: YahooMailRC/397.8 YahooMailWebService/0.8.103.269680
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="0-1661809515-1276368089=:83440"
Content-Length: 612

Hi Support Services,

My Etoken is completed locked up and I forgot the password. I am really sorry... I need my Etoken and password reset. Below is the challenge data

4E 2B 63 A3 5B 3C 2B D2

Please let me know what's my new password is. Please, it's no hurry, whenever you get a chance today to unlock it so I can work from my hotel tomorrow. Just email me the response data and new password. I should be able to enter them in my etoken property, and with the new password.

Thanks you and enjoy your weekend.

John Bare

and then...

Subject: Re: Etoken locked up..
From: John Bare <john.baregucci@yahoo.com>
Date: Sat, 12 Jun 2010 13:01:30 -0700 (PDT)
To: Support.Services@us.gucci.com
X-RocketMail: 00000002;R---S-----;2890
X-Mail-OSG: 7tQewLsVM1nS14bPf0deWpPwVd9q8TLpPzlbCem4AM0vq4M
n8Hy_GHxeWFPZz5qhF5X.I54ATG8suUVXJYFODm1q1aaeNa52anm8wG7qjRO
IfBET6hg864PYKjBVHrbKo0Brux1GUbnNcHkpu5PqW19E0gZF2dYY4YHUCS
_J7ZnCWramh0805RIIYFZqCa4MBrgxQlqzwfKSE1fZJ.GCO4URu1EryqNlsl
O0EoEKtO2vTRW02_8O94kaTBkQKAawVez9cyUWoy0afwhHQQVInyallCgjk.IGleXhA--
Received: from [98.113.222.37] by web114504.mail.gq1.yahoo.com via HTTP; Sat, 12 Jun 2010
13:01:30 PDT
X-Mailer: YahooMailRC/397.8 YahooMailWebService/O.8.103.269680
References: <OF34100BAA.C8382D7C-
ON85257740.00670A87-85257740.00675430@guccigroup.com>
In-Reply-To: <OF34100BAA.C8382D7C-
ON85257740.00670A87-85257740.00675430@guccigroup.com>
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="0-595203991-1276372890-25133"
Content-Length: 1788

Hi Mike,

I really appreciate your prompt reply! I am at my hotel in Mexico City, preparing for an event tonight. I will leave my computer up and the Etoken window up as well. Please don't go out of your way for this as I will be in and out for the most part for the occasion tonight. I just need it by tomorrow to log into my Notes to check emails. Believe it or not, the reception here is terrible and I can't get any international calls here.

Thanks again Mike! I really appreciate it.

Gucci Network Attack

- Yin was charged with First Degree Computer Tampering, and Computer Trespass, among other charges
- Yin pleaded guilty in July 2012
- Yin was sentenced to 2-6 years state prison time



Beyond Service Disruption...

Hacks often involve theft of payment information, usually credit and debit card information



Hacks: Theft of Payment Information



And it doesn't end there...

Michaels

TJ-maxx

Hilton

Neiman Marcus

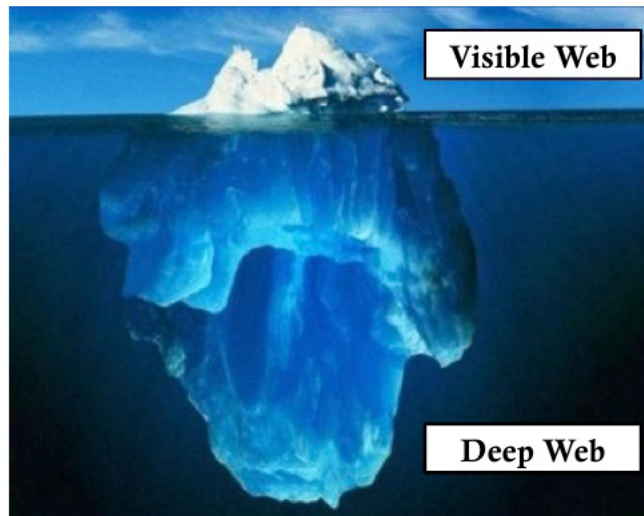
Marshalls.

Marriott

What happens to stolen credit card data?

- Numbers are bundled in bunches and sold on carding forums such as Carderplanet and Mazafaka
- For very little money, you can obtain a stolen credit card number, expiration date and CVV code
- These forums and virtual storefronts exist on the Deep Web aka “Dark Web” or “Undernet”

Deep Web



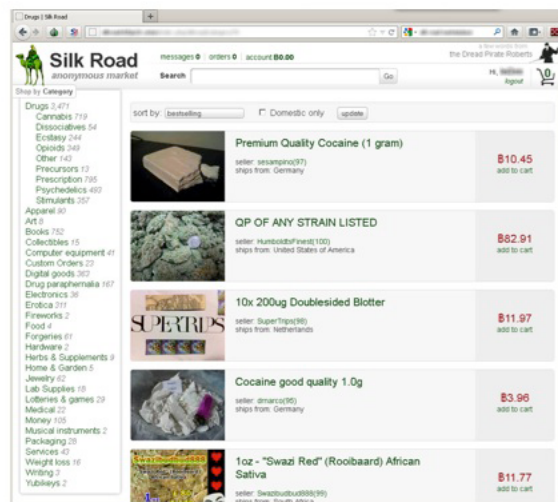
Deep Web

- Utilizes a matrix of encrypted websites that allow users to surf beneath the everyday Internet with complete anonymity
- Use digital currencies and exchanges such as e-Gold, WebMoney, and BitCoin
- Widely used for criminal activity
 1. Purchase illegal drugs, weapons and explosives
 2. Hire a hit-man
 3. Obtain child pornography
 4. Human trafficking



Deep Web: Silk Road

- Online marketplace where users can purchase goods, often illegal, without web traffic monitoring
- The “eBay” or “Amazon” for drugs
- 10/2/2013: FBI shuts it down and arrests Ross William Ulbricht
- 11/6/2013: Silk Road 2.0 launched



Carding Forums:

Please start accepting Bitcoins if you want more deals...

Omerta.pw - Jabber server without LOGS

**24 HOURS SUPPORT
AND UPDATE EVERY DAY!**

Omerta.cc - many SERVICES + 17.000 more USERS! DUMPS, CVV, CASHING for Brothers! Popular CARDING FORUM for YOU! Best place for carders!

Carding Forum - English speaking carders - Pleading & Offshore
An open suggestion to all vendors and others!

User Name: Password: Remember Me? ☐

[Reply]

15/08/2015, 05:21 PM
Lucy - Review

Please start accepting Bitcoin if you want more deals.
Bitcoin is a peer-to-peer currency. Peer-to-peer means that no central authority issues new money or tracks transactions. These tasks are managed collectively by the network.

Pros:

- No chargebacks
- Anonymous if you know what you are doing
- No need to register accounts or that bullshit
- Safe and secure if you know what you are doing
- No central authority so no one will suspend your account
- etc.

Cons:

- Not very stable but this is changing as more people use it.

It is already accepted largely in the "deep web" and on onion hidden sites, which contains users for more technology savvy than on here and most carding forums.

Find out more at Bitcoin.org

Please, vendors, consider accepting it as a currency! Let's get rid of Liberty Reserve/Worldmoney which suspended our accounts with their strict policies without real reasons!

Open discussion.

Click the links below to read some good articles - cool:

Carding related websites by me

Omerta Track 1 Generator

Omerta - Carding Forum, Buy Dumps & Credit Cards

Shadowcrew :: Просмотр темы - over 2 million DUMPS for sale. every month fresh dumps !!! - Mozilla Firefox <2>

File Edit View Go Bookmarks Tools Help

http://63.240.81.5/phpBB2/viewtopic.php?t=4683&gb=TRUE

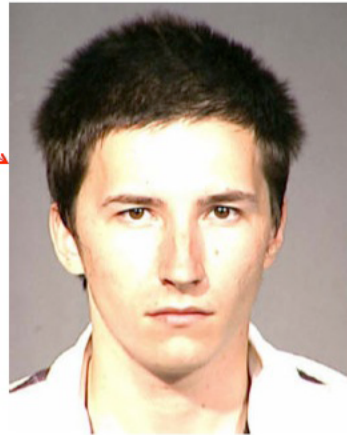
over 2 million DUMPS for sale. every month fresh dumps !!!
На страницу 1, 2 След.

NEW TOPIC POST REPLY Список форумов Shadowcrew -> Global Forum -> Vendors/Reviews

Предыдущая тема :: Следующая тема

Автор	Сообщение
Eskalibur Reviewed Vendor	Добавлено: 8c Aer 15, 2004 5:15 am every month fresh dumps !!! Зарубочек сообщения: over 2 million DUMPS for sale.
Зарегистрирован: 04.11.2003 Сообщений: 55 Откуда: dumps.ru	NEWS 30.08.2004 Got tons fresh canadian dumps, only second tracks. 90% dumps coming with real first track. they are NOT generated. USA DUMPS ● Visa Classic, mastercard standart 10-50 - 20\$/dump 50-100 - 15\$/dump over 100 - 10\$/dump ● Visa Gold/Platinum/Signature/Purchasing/Business/Corporate 10-50 - 38\$/dump 50-100 - 33\$/dump over 100 - 27\$/dump ● Mastercard except standart(premiere/etc) 10-50 - 38\$/dump 50-100 - 33\$/dump over 100 - 27\$/dump EUROPE: visa Gold/Platinum/Signature/Purchasing/Business/Corporate 150\$ per dump (france, spain, italy, turkey -160\$ per dump) mastercard - 100\$ per dump (france, spain, italy, turkey -120\$ per dump) visa classic - 75\$ (france, spain, italy, turkey -100\$ per dump)

Автор	
Eskalibur	■ Доб
Reviewed Vendor	every
Зарегистрирован: 04.11.2003	30.08
Сообщения: 55	
Откуда: dumps.ru	



But who's Eskalibur?

People v. Western Express

- Shevelev, now 27 years old, trafficked in over \$5 million in stolen credit card numbers, facilitated in part by an illicit entity known as Western Express.
- Shevelev used email accounts including uschenko@gmail.com and ussrchencko@gmail.com to sell card dumps to his clients.



Unraveling Cyber Anonymity

DATE/TIME [Eastern]	FROM	TO	SUBJECT	ATTCH
5/4/2008 19:39	ussrchenko@gmail.com	glennsmoth@yahoo.com	+Auto Reply+ Re: any news?, today is sunday"	
5/4/2008 19:47	ussrchenko@gmail.com	badma43@yahoo.com	+Auto Reply+ Re:	
5/4/2008 23:40	usschenko@gmail.com	arvisujoel@hotmail.com	Re: order	
5/4/2008 23:48	ussrchenko@gmail.com	nothingladdy@yahoo.com	Re: you already have wu	*
5/4/2008 23:50	ussrchenko@gmail.com	Foxnogoraj@yahoo.com	+	
5/5/2008 6:51	ussrchenko@gmail.com	819966@gmail.com	=+Auto Reply+ Re: from: mic3652407	
5/5/2008 7:55	ussrchenko@gmail.com	zodollatmail.com	+Auto Reply+ Re: +Auto Reply+ Re: Dld u get funds	

5/ Re: order

Subject: Re: order
From: "Anton Antonovich" <uschenko@gmail.com>
Date: Mon, 5 May 2008 06:40:23 +0300
To: "joel jose arvisu" <arvisujoel@hotmail.com>

ssory for delay, due holidays will be ready next monday

Unraveling Cyber Anonymity

+Auto Reply+ Re: НУЖЕН HOMEP КОШЕЛЪКА!!!!

DATE/
[East

5/4/2008

5/4/2008

5/4/2008

5/4/2008

5/4/2008

5/5/2008

5/5/2008

Subject: +Auto Reply+ Re: НУЖЕН HOMEP КОШЕЛЪКА!!!!

From: "Anton Antonowitch" <ussrchenko@gmail.com>

Date: Mon, 5 May 2008 09:39:36 -0700

To: hotpepper98@gmail.com

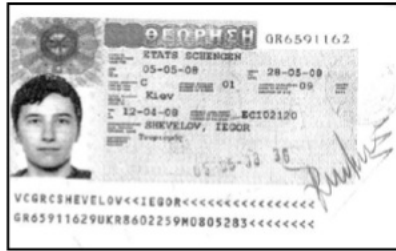
I am on holidays till 13.05 then I will process all your orders in nearest time.

Dear friends, ssory if your order is not ready yet.

5/5/2008 9:28	ussrchenko@gmail.com	glennsmoth@yahoo.com	=+Auto Reply+ Re: what is going on?	
5/5/2008 12:39	ussrchenko@gmail.com	hotpepper98@gmail.com	+Auto Reply+ Re: ДДfD-D•D ДDfDαD•D ДDfD"D•D-D-DfD!!!!	
5/5/2008 13:56	ussrchenko@gmail.com	guttcheckin@yahoo.com	+Auto Reply+ Re: ???yooco	
5/5/2008 17:56	ussrchenko@gmail.com	badma43@yahoo.com	+Auto Reply+ Re: +Auto Reply+ Re:	
5/5/2008 23:32	ussrchenko@gmail.com	bigbizok@hushmail.com	=+Auto Reply+ Re: Order info	
5/6/2008 2:04	uschenko@gmail.com	uschenko@gmail.com	Subject: Can you imagine of being healthy.Dear us	

Unraveling Cyber Anonymity

Shevelev was out of the country on May 5, 2008



Above:
Shevelev's passport
is stamped May 5, 2008



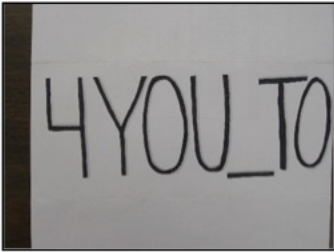
People v. Western Express

- Shevelev sold card numbers to individuals, including Latta and Ciano in New York, who forged cards and used them to purchase goods, such as Apple products, and to fence them, primarily on eBay.

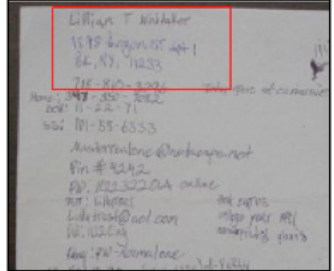



People v. Western Express

Documents found in Latta and Ciano's Brooklyn apartment identified them as the users of eBay and PayPal accounts used to fence goods.


→

Registration Information	
Name:	whitaker Lill
User ID:	4you_to
Email:	willwhit@aol.com
Address:	230 4th ave
City, State:	New York, NY
Zip:	10002
Country:	US
Day Phone:	347 625 1232
Date of Birth:	1/10/1971 7:00:00 AM
Reg IP:	24.190.192.174
Date Registration:	23/March/2007 GMT


→

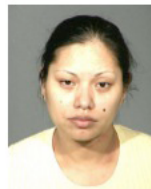


FIT Page for Lillian whitaker

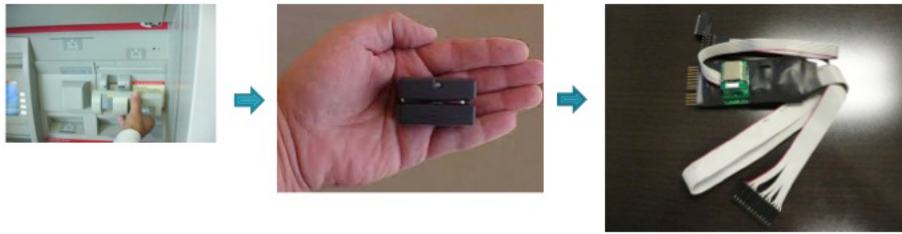
User Info	
First Name:	Lillian
Last Name:	whitaker

People v. Western Express

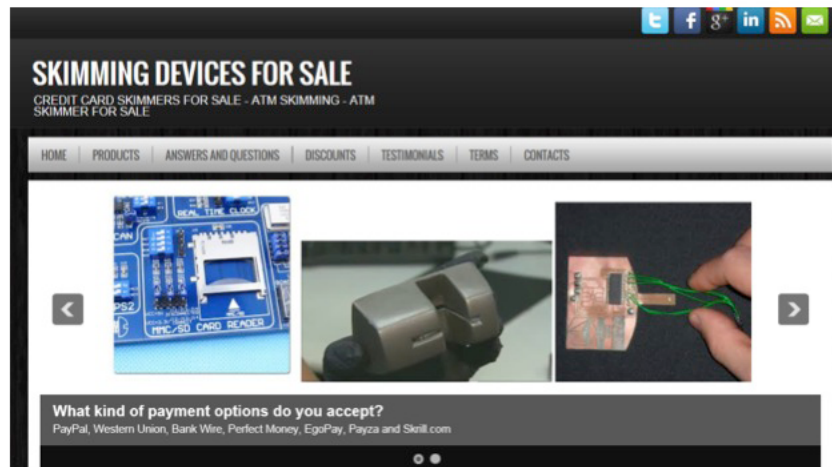
- Defendants convicted after trial of Grand Larceny, Criminal Possession of Stolen Property, Scheme to Defraud, and Conspiracy in June 2013
- Sentencing:
 - Shevelev sentenced to 14 to 40 years state prison
 - Latta sentenced to 22 to 44 years state prison
 - Ciano sentenced to 20 to 47 years state prison



Other Ways to Steal Data: Skimming Devices



Other Ways to Steal Data: Skimming Devices



Skimming: Handheld Devices

- NYPD and DANY have arrested and prosecuted skimmers at many Manhattan retailers



Coast to Coast Cash-Out

- Skimming devices placed inside gas pumps in Texas
- Payment information collected and distributed to cells
- Cards were encoded with the stolen credit card data
- Criminals came to New York to “cash-out”
- Cash was then deposited in New York and withdrawn primarily in California

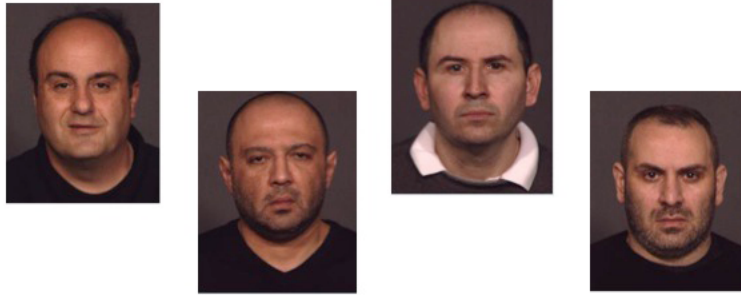
Coast to Coast Cash-Out

- Police Officer observes 2 individuals inside an ATM vestibule
- Search Warrant of hotel room produced a re-encoding machine, blank cards, and approximately \$300,000 in cash



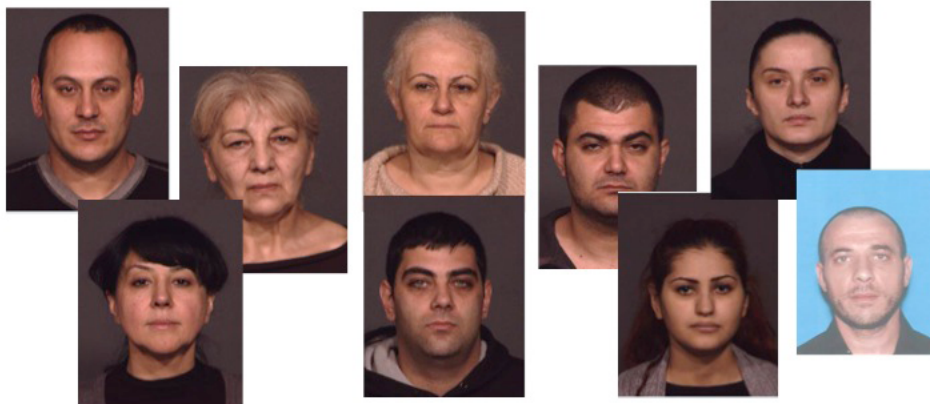
Coast to Coast Cash-Out

- 4 charged with Grand Larceny and Money Laundering in January 2014
- Case pending in New York State Supreme Court

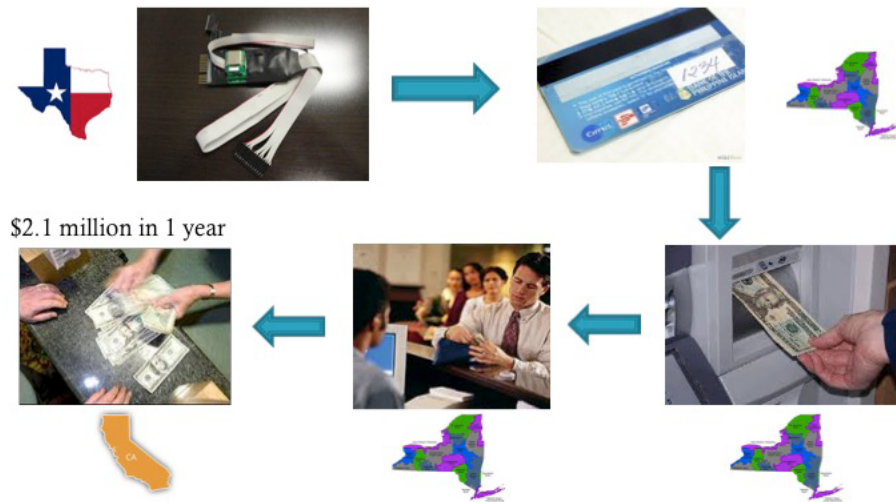


Coast to Coast Cash-Out

- 9 others charged with Money Laundering
- Case pending in New York State Supreme Court



Coast to Coast Cash-Out



The Threat Landscape

1. Hacking of Computer Networks, Systems, and Databases
2. Theft of Personal Identifying Information
3. Intellectual Property Theft



What data is being stolen?

Personal Identifying Information

- Email Username and Password
- Bank Account Information
- Computer System Password
- Date of Birth
- Social Security Number
- Mother's Maiden Name



Personal Identifying Information Theft

Old-fashioned approach:

- Employees of organizations that store your personal identifying information, copy or otherwise steal the data
- Common points of compromise:
 - Doctor's Offices
 - Human Resource Departments
 - Nursing Homes
 - Banks
 - Hospitals

Personal Identifying Information Theft

- Brute Force Attack
- Phishing Approach



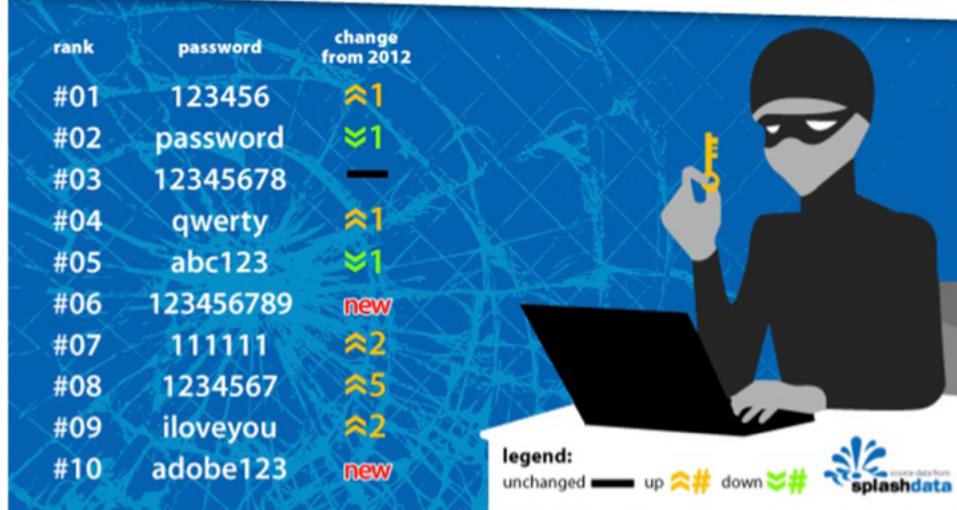
How to do Hydra (Brute force Attack) to hack any E-mail Password

POSTED ON 3/25/2013 12:30:00 PM BY VIV EK



A password attack that does not attempt to decrypt any information, but continue to try different passwords. For example, a brute-force attack may have a dictionary of all words or a listing of commonly used passwords. To gain access to an account using a brute-force attack, a program tries all available words it has to gain access to the account. Another type of brute-force attack is a program that runs through all letters or letters and numbers until it gets a match.

WORST PASSWORDS OF 2013



Phishing Emails

From: Orders
Sent: Wednesday, November 06, 2013 8:34 AM
Subject: Re: Order Placed at [REDACTED]

Thank you for shopping at [REDACTED]. Before your order will be shipped, it is required that you confirm the your credit card information by replying this email with the requested details below;

Type of Card:
Card Number:
Name on Card:
Billing Address:
Expiring Date:
CVV:

We will dispatch your order immediately we receive the details.

Phishing Emails



Internal Revenue Service IRS.gov
DEPARTMENT OF THE TREASURY

DECEMBER, 2013

Dear Sir

Our records indicate that you are a non-resident alien. As a result, you are exempted from United States of America Tax reporting and withholdings, on interest paid on your account and other financial dealing to protect your exemption from tax on your account and other financial benefit in rectifying your exemption status.

Therefore, you are to authenticate the following by completing form W-8BEN, and return to us as soon as possible through the fax number:

If you are a USA Citizen and resident, this form W-8BEN is not meant for you, please indicate "USA Citizen/Resident" on the form and return it to us. We shall then send you a form W9095.

When completing form W-8BEN, please follow the steps below

1. We need you to provide your permanent address if different from the current mailing address on your Form W-8BEN; you must indicate if a non-USA resident, your country of origin to support your non-resident status (if your bank account or other financial dealing has a USA address for mailing purpose).
2. If any joint account holder are now USA residents or Citizen, or in any way subject to USA tax reporting laws, Please check the box in this section.
3. Please have all account holders, sign and date the form separately and fax it to the above-mentioned number.

Please, complete Form W-8BEN "attached" and return to us within 1 (one) week from the receipt of this letter by faxing it, to enable us update your records immediately if your account or any other financial benefits are not rectified in a timely manner, it will be subject to USA tax reporting and back up withholding (if back up withholding applies, we are required to withhold 30% of the interest paid to you).

We appreciate your cooperation in helping us protect your exempt status and also update our records.

Sincerely,


Kevin Smith
Director of Information

Phishing Emails

From:
To:
Date: 11/18/2013 02:04 PM
Subject: Wire instruction

Hi

This wire instruction is urgent, kindly debit my account with \$8,000 and credit the following bank account;

Bank Name: Bank of America
Account number: 00343
Routing number: 026009593
Beneficiary name:

Kindly treat as urgent and confirm to me when the wire has been completed.

Thanks

**And once the cybercriminal has
hooked your personal identifying
information...**



How is a stolen identity used?

- Obtain new credit accounts in victims' names



How is a stolen identity used?

- Obtain instant credit



How is a stolen identity used?

Secure Credit Card Application - Barclaycard

9/3/12 12:22 AM

Thank you!

Instant Credit

Please bring your Instant Credit barcode to any Apple Retail Specialist to make a purchase using your new credit card account. You will need to provide your driver's license for identification.

VALID FOR 10 DAYS ONLY

Issued on: 09/03/2012 Authorized Initial Purchase Amount: \$3,500.00 Acct #: 
Expiration Date: 

VALID FOR 10 DAYS ONLY

Important Information Regarding Your New Account

Your new credit card account qualifies you to receive a special interest rate offer on your Apple Store purchases made within 30 days of account approval. To take advantage of this offer before your card arrives, you must keep a copy of this barcode and use it within 10 days from your account issue date. You may use this barcode multiple times, however, it is only good for 10 days starting on the date of issuance and only valid at Apple Stores.

If you do not wish to make a purchase within 10 days, you must wait until you receive your credit card in the mail to make your first purchase. Your card will arrive in approximately 7-10 business days.

Apple Store Employees: If you have difficulty scanning the barcode, please call the Barclaycard US Technical Support line at 1-866-609-2761.

How is a stolen identity used?

- Steal from your bank account

From:	Chris [REDACTED]	Sent:	Mon 1/13/2014 12:30 PM
To:	Ryan [REDACTED]		
Cc:			
Subject:	Re: Inquiry		

Ryan i would like you to complete a wire transfer for me today. total of \$9600. for a business purpose.. kindly confirm for me how much the charges and what do i need to do.

Chris

- Generate fraudulent tax returns and obtain instant tax refunds

when you direct deposit it to your Green Dot card

Just log in to your Green Dot account then enter your direct deposit information onto your tax return.

PLEASE LOGIN
TO VIEW INFORMATION

It's simple!
Just log in to your Green Dot account then enter your direct deposit information onto your tax return.

PLEASE LOGIN TO VIEW INFORMATION

Refund

71 Credits from Form: **a** 2439 **b** Reserved **c** 8885 **d** 1099-R

72 Add lines 62, 63, 64a, and 65 through 71. These are your total payments

73 If line 72 is more than line 61, subtract line 61 from line 72. This is the amount you overpaid

74a Amount of line 73 you want refunded to you. If Form 8888 is attached, check here

Direct deposit? **b** Routing number **YOUR NUMBERS GO HERE** **c** Type: ☒ Checking ☐ Savings

See instructions. **d** Account number

75 Amount of line 73 you want applied to your 2014 estimated tax

Amount You Owe

76 Amount you owe. Subtract line 72 from line 61. For details on how to pay, see instructions

77 Estimated tax penalty (see instructions)

Do you want to allow another person to discuss this return with the IRS (see instructions)? **Yes** **No**

Print
Preparer Use Only
Date
Preparer's signature
Signature
Date

People v. Murmylyuk

- Peter Murmylyuk created a fake job placement website where he stole the personal identifying information of more than 300 people
- Used that information to file more than 100 fraudulent federal income tax returns in their names
- Stole more than \$450,000 in taxpayer money

People v. Murmylyuk

Career Services admin@contractor.net

A government sponsored employment agency has a few vacancies for entry level Office Clerk part time position under the new government program for students who made too little money last year to file taxes.

So, ONLY STUDENTS WHO DIDN'T FILE THEIR TAXES FOR THE YEAR 2010 (for any reason) qualify, it will be verified.

Following qualities are sought:

- Well organized
- Ability to multitask
- Ability to work consistently and effectively with minimal or no supervision
- Interact with clients as necessary in a professional manner
- Demonstrated self-starter who takes initiative when needed
- Detail oriented, organized, team player
- Strong attention to details

\$28 per hour. 20 hours per week.

Please fill out the application and one of our advisors will contact you within 24 hours.

<http://jobcentral2.net/govapply/start/app.html>

Phishing Email

People v. Murmylyuk

Fake job placement
website:

www.jobcentral2.net

The job program is sponsored by the government and intended for people with low income.
Only those who didn't file their taxes for 2010 due to little or no income are qualified!

[View information in pdf and audio](#)

JOB APPLICATION

Personal Information

First Name
Last Name
Social Security Number
Date of Birth (MM/DD/YYYY)
Email Address
Mail/Other Contact Address

Address Information

Current Address
City
State
Zip Code
Home or Cell Phone Number

Law Information

Did you file taxes for year 2009?
Did you file taxes for year 2008?
Have you earned an income in year 2009?

Consent to Electronic Information (2008 & 2009)

You may not delete either address and accept these disclosures and information electronically.


By clicking on "Yes" you may receive other information, such as collection notices or other legal notices electronically. You will be able to unsubscribe at any time.

☐ I consent to receive information electronically.

It is our goal to offer you the job that best fits your profile.

[Continue Application](#) [Cancel Application](#)

If you're experiencing technical difficulties while applying for our website, please call Technical Support at 1 (877) 272-2722 about 9am to 5pm ET, Monday through Friday.

 about the government

Copyright © 2007 Job Central Corporation. All Rights Reserved.

People v. Murmylyuk

- Sentenced this month in New York State Supreme Court to 3 to 9 years state prison on Grand Larceny and Money Laundering charges



The Threat Landscape

1. Hacking of Computer Networks, Systems, and Databases
2. Theft of Personal Identifying Information
3. Intellectual Property Theft



Intellectual Property Theft: Goldman Sachs Programmer

- Goldman Sachs created its high-frequency trading system that performs sophisticated high-speed and high-volume trades on various stock and commodity
- Sergey Aleynikov, a computer programmer employed by Goldman Sachs, transferred hundreds of thousands of lines of trading source code to a foreign server on his last day of employment



Intellectual Property Theft: Goldman Sachs Programmer

- In December 2010, Defendant charged and tried by the federal government for theft of trade secrets and transportation of stolen property
- Sentenced to 97 months and 3 years supervised release
- In February 2012, Second Circuit reversed his conviction, after being incarcerated for over a year



Intellectual Property Theft: Goldman Sachs Programmer

- In August 2012, Manhattan District Attorney's Office rearrested and charged Aleynikov with Unlawful Use of Secret Scientific Material and Unlawful Duplication of Computer Related Material
- Case pending in New York State Supreme Court



Intellectual Property Theft: Flow Traders

- Flow Traders, LLC is an Amsterdam-based proprietary trading house which trades a range of stocks and commodities worldwide
- A trader at the firm, JASON VUU, emailed himself trading strategies and valuation algorithms before resigning in March 2013 to start their own trading entity
- VUU disguised the stolen data by changing the file extensions of email attachments

Intellectual Property Theft: Flow Traders

- VUU worked with a college friend and third defendant, SIMON LU, to create a trading platform for a potential startup company
- The investigation revealed that the defendants used Dropbox and other cloud based sharing services to share the stolen data

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK

IN THE MATTER OF AN APPLICATION PURSUANT TO C.P.L. ARTICLE 690 AND 18 U.S.C. § 2703 FOR A WARRANT ORDER TO SEARCH OBTAIN RECORDS RELATING TO THE GOOGLE (A.K.A GMAIL.COM) ACCOUNTS ASSOCIATED WITH THE FOLLOWING EMAIL ADDRESSES:
(1) JOHNSMITH@GMAIL.COM,
(2) JOHNDOE@GMAIL.COM, AND
(3) JANEDOE@GMAIL.COM AND AN ORDER DIRECTING THE SERVICE PROVIDER TO REMOVE USER ACCESS FROM THE ABOVE EMAIL ADDRESSES ("THE TARGET EMAIL ADDRESSES"), AS WELL AS

ORDERS TO REMOVE USER ACCESS FROM THE BITBUCKET.ORG ("BITBUCKET") ACCOUNTS WITH USER NAMES JOHNSMITH AND THE DROPBOX.COM ("DROPBOX") AND BITBUCKET ACCOUNTS ASSOCIATED WITH THE FOLLOWING EMAIL ADDRESSES:
(1) JOHNSMITH@GMAIL.COM,
(2) JOHNDOE@GMAIL.COM, AND
(3) JANEDOE@GMAIL.COM ("THE TARGET ACCOUNTS")

AFFIDAVIT IN SUPPORT OF
SEARCH WARRANT

Investigator John Stopcrime, being duly sworn, deposes and says:

Intellectual Property Theft: Flow Traders

- Defendants charged in July 2013 in an indictment in New York State Supreme Court with multiple counts of Unlawful Duplication of Computer Related Material and Unlawful Use of Secret Scientific Material
- Case pending in New York State Supreme Court

FLOW ■ TRADERS

Cyberattacks and Universities

The New York Times

July 16, 2013

Universities Face a Rising Barrage of Cyberattacks

By RICHARD PÉREZ-PEÑA

America's research universities, among the most open and robust centers of information exchange in the world, are increasingly coming under cyberattack, most of it thought to be from China, with millions of hacking attempts weekly. Campuses are being forced to tighten security, constrict their culture of openness and try to determine what has been stolen.

Bill Mellon of the University of Wisconsin said that when he set out to overhaul computer security recently, he was stunned by the sheer volume of hacking attempts.

"We get 90,000 to 100,000 attempts per day, from China alone, to penetrate our system," said Mr. Mellon.

"A university environment is very different from a corporation or a government agency, because of the kind of openness and free flow of information you're trying to promote," said David J. Shaw, the chief information security officer at Purdue.

Universities and their professors are awarded thousands of patents each year, some with vast potential value, in fields as disparate as prescription drugs, computer chips, fuel cells, aircraft and medical devices.



Sophi Jacobs
Assistant District Attorney
(212) 335-9144
jacobss@dany.nyc.gov



PEOPLE

Linn Foster Freedman
Kathryn M. Sylvia

SERVICES

Data Security & Breach Response
Privacy & Data Protection
Privacy Litigation & Enforcement Actions

Alerts/Articles

What's trending in data privacy & security

July 25, 2014

Privacy Alert

Author(s): Linn Foster Freedman, Kathryn M. Sylvia

We're looking ahead on all fronts in data privacy and security. The NY attorney general releases a detailed report outlining an analysis of data breaches reported between 2006 and 2013. And a career planning company settles a \$2.6 million class action suit for sending unsolicited promotional faxes. Are your marketing messages TCPA compliant? Here's a round-up of the latest news.

Data breach

Florida bank suffers cyberattack, exposing over 72,500 customers' personal and financial information

TotalBank, located in South Florida with over 21 branches, experienced a hack of its computer network on June 24, 2014, that exposed account information of over 72,500 customers, including name, address, bank account numbers and balance, Social Security numbers, driver's license numbers, passport numbers and alien registration numbers. The bank notified the customers of the incident on July 17, 2014, after it had been discovered. TotalBank released a statement indicating that the breach will not permit the third-party hacker to access customer bank accounts because no passwords or access information was compromised. It has mitigated the breach with reinforcement of firewalls, better threat detection and closed access to the compromised systems. However, the investigation into the breach continues as TotalBank works alongside law enforcement to determine the root of the cyberattack. With the stringent breach notification law in Florida, TotalBank had only 30 days to notify consumers of this hack once it discovered the breach, but it now stresses that its systems are secure and encourages its customers [to visit its website](#) for more information on security breaches.—*Kathryn M. Sylvia*

NY attorney general reports a record number of data breaches in 2013

This week, New York Attorney General Eric Schneiderman (NYAG) issued a comprehensive report on data breaches entitled "[Information Exposed: Historical Examination of Data Breaches in New York State](#)." This well-done and detailed report outlines an analysis of data breach notifications to the NYAG's office between 2006 and 2013. We highly recommend that you take the time to read the report as, in our experience, it is very representative of data breaches occurring all over the country and has a wealth of information that is useful to individuals, businesses and government.

The key findings are that between 2006 and 2013, reported security breaches in New York tripled and the "number of victims in New York has exploded." The report indicates that over 22.8 million New Yorkers' personal information has been exposed since 2006. The statistics outlined in the report also include that 2013 was a record-breaking year of data breaches as more than 7.3 million New Yorkers' records were exposed, costing businesses approximately \$1.37 billion (yes, that's "billion" with a "b"). Five of the ten largest breaches occurred in the last three years, and hacking accounted for over 40% of all data breaches between 2006 and 2013.

accounted for over 40% of all data breaches between 2009 and 2013.

The NYAG states “organizations can do more to prevent . . . breaches, such as insider wrongdoing and inadvertent disclosures, by ensuring that they have the best data security practices in place. This report provides recommendations that individuals and organizations can implement to protect themselves from data loss.”

Good for the NYAG, who concludes that because the data breach problem is so complex, he is calling for a systemic response and advocating for a pro-active collaborative approach between industry stakeholders, security experts and lawmakers to work together to help individuals and businesses with tools and information needed to promote best data security practices.—*Linn Foster Freedman*

Goodwill Industries International Inc. investigating possible data breach

Goodwill Industries International Inc. posted on its website this week that it is investigating a possible data breach as a result of being notified that the credit card numbers of its customers in reportedly over 21 states may have been exposed since 2013. Although the investigation is pending, this is another stark reminder that all companies, big and small, profit or nonprofit, must make data security its top priority from C-Suite and board down throughout the organization.—*Linn Foster Freedman*

Cybersecurity

GAO report: FDIC's security measures expose financial data to risk

The U.S. Government Accountability Office (GAO) recently released “[Information Security: FDIC Made Progress in Securing Key Financial Systems, but Weaknesses Remain.](#)” a report after an audit of the Federal Deposit Insurance Corporation’s (FDIC) information security systems. The report states that the systems continue to expose sensitive financial information to unnecessary risk.

In 2012, the GAO audited the FDIC’s systems and reported that the FDIC had 39 security weaknesses that needed to be addressed. Although the FDIC is making progress on these security measures, the most recent audit found that the FDIC has not fully implemented security controls for authentication of users, restricting access to sensitive data, encryption technology and auditing and monitoring standards, which exposes the FDIC’s sensitive financial information to “unnecessary risk of inadvertent or deliberate misuse, improper modification, unauthorized disclosure, or destruction.”

The GAO provided four recommendations to the FDIC to improve its security measures, which included improved documentation, ensuring that all employees and contractors receive security awareness training, conducting ongoing assessments of security controls and addressing security weaknesses in a more timely fashion. The FDIC has committed to complete measures to address the four recommendations by December 31, 2014.

The GAO stated “Given that federal agencies face an evolving array of cyber-based threats to information and information systems and that attackers have a variety of increasingly sophisticated attack techniques at their disposal, it is vitally important that FDIC address the remaining weaknesses in information security controls—both old and new.”—*Linn Foster Freedman*

Data privacy

Truncated taxpayer ID numbers allowed in IRS final rules combating identity theft

Last week, in an effort to combat identity theft, the IRS issued final rules (TD9675) (“the Rules”) allowing truncated tax identification numbers (TTIN) on certain statements issued to payees. The Rules allow businesses issuing payee statements to 1099 contractors, a retirement or pension plan participant receiving distributions, a transferor of real estate, a payer of mortgage interest, a debtor who has cancellation of debt income or a student receiving scholarships, qualified tuition or grants to truncate

the full Social Security number or other tax identification number to the first five digits, and then Xs or asterisks for the remainder of the numbers on any electronic or paper payee statements. Generally, the Rules are effective for payee statements due after December 31, 2014.

Although this is a good start by the IRS to combat identity theft, unfortunately, the Rules do not allow a TTIN to be used on W-2 statements issued to employees, by an individual taxpayer on a tax form, on a W-9 form or for an employer to truncate its EIN on W-2 forms furnished to employees. Until there is a way to eliminate the mailing or sending of full Social Security numbers or other taxpayer identification numbers on IRS forms through unsecure electronic transmission, the risk of identity theft will remain a real issue for taxpayers.—*Linn Foster Freedman*

Enforcement & litigation

Sutter Health prevails in appeal of \$4 billion data breach class action

Sutter Health scored a huge win this week after a California appeals court reversed a decision holding it potentially accountable for a data breach involving the personal and health information of 4.3 million patients. The breach occurred when a computer was stolen, which contained a database that included the names, addresses, dates of birth, telephone numbers, e-mail addresses, medical record numbers and names of health insurance plans of 3.3 million individuals. The computer did not contain any patient financial information, Social Security numbers or health insurance numbers or information for those 3.3 million individuals, but did contain dates of service and descriptions of diagnoses for another 1 million individuals.

Following notification of the computer theft, plaintiffs filed a class action lawsuit seeking statutory damages of up to \$1,000 per individual for the 4.3 million patients. The lower court found that Sutter Health could be liable under the California Confidentiality of Medical Information Act. Sutter Health appealed and the California appeals court reversed the decision holding that Sutter Health could not have violated the California Confidentiality of Medical Information Act because there was no evidence that the thief who stole the computer had actually viewed any of the information. The court further held that “the mere possession” of the records was not enough to violate the law, and because the class had not provided any evidence that the information was even viewed, the case should have been dismissed. It noted that although the complaint alleged potential misuses of the information, it did not state a claim because the plaintiffs failed to allege an actual breach of the confidentiality of the information. This is a significant decision that is consistent with many other jurisdictions that the mere loss of information does not form the basis for a claim for monetary damages. We are following these cases closely and will continue to report on them as they are decided.—*Linn Foster Freedman*

Women & Infants Hospital settles with MA AG over data breach

Women & Infants Hospital of Rhode Island (“WIH”) settled with the Massachusetts attorney general on July 23, 2014, for its alleged failure to effectively protect and secure personal and health information of more than 12,000 Massachusetts residents. In 2012, WIH lost 19 unencrypted backup tapes from its Prenatal Diagnostics Center in Providence, Rhode Island, while transporting the backup tapes. The backup tapes contained patient’s names, dates of birth, Social Security numbers, dates of medical exams, treating providers’ names and health information, such as ultrasound images. It notified the Massachusetts Attorney General of the data breach in November 2012 in accordance with Massachusetts’s breach notification law and has settled with the attorney general for a \$110,000 civil penalty, \$25,000 for attorneys’ fees and costs, and \$15,000 to the attorney general fund for education on protecting personal and health information. WIH has also agreed to revise its data privacy and security practices, after auditing its current safeguards. This case illustrates how important it is to ensure that any protected health information that is transported off site, including back-up tapes, are properly protected through encryption or other secure means.

—Kathryn M. Sylvia and Linn Foster Freedman

Career planning company settles TCPA class action for \$2.6 million for over 10,000 unsolicited fax ads

On July 18, 2014, a New Jersey federal court approved a class action settlement of \$2.6 million with Peterson's Nelnet LLC ("Nelnet") for its alleged violations of the Telephone Consumer Protection Act (TCPA). Nelnet provides college and career planning, and it was alleged by the class that Nelnet sent over 10,000 unsolicited fax advertisements for their services and programs without prior express written consent as required by the TCPA. Nelnet stated that it decided to settle the litigation because TCPA actions often result in complex legal issues and could result in high expenses for the company. The \$2.6 million settlement amount will first go toward attorneys' fees and then the balance of the fund will be distributed and prorated on the amount that each class member would have otherwise been awarded if the amount is not enough to pay all valid claims. If any amount is left over after Nelnet has paid off all of its dues under the settlement agreement, Nelnet will receive the additional funds back. Nelnet has additionally agreed to a permanent injunction that prohibits it from sending fax solicitations in violation of the TCPA. The lesson: no matter the media, be sure your business is sending marketing messages in compliance with federal regulations to avoid large settlements like this.—Kathryn M. Sylvia

Ideas

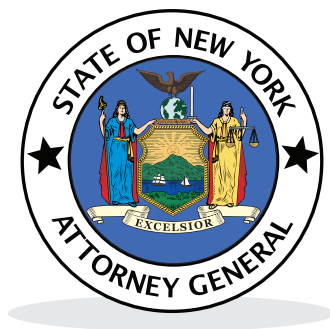
What's trending in data privacy & security
Privacy Alert | July 18, 2014

What's trending in data privacy & security
Privacy Alert | June 13, 2014

The foregoing has been prepared for the general information of clients and friends of the firm. It is not meant to provide legal advice with respect to any specific matter and should not be acted upon without professional counsel. If you have any questions or require any further information regarding these or other related matters, please contact your regular Nixon Peabody LLP representative. This material may be considered advertising under certain rules of professional conduct.

INFORMATION EXPOSED

Historical Examination of Data Breaches in New York State



From the Office of:

New York State Attorney General
Eric T. Schneiderman

Dear Fellow New Yorker,

Every day, New Yorkers share personal information with companies, government agencies, and other organizations, either out of necessity or simply for the sake of convenience. When we do, we trust these institutions to protect our sensitive data from unauthorized access. That is why New York has a data breach notification law. If an unauthorized individual accesses your personal information, the institution that suffered the data breach must notify you, as well as my office, as soon as possible. An institution that fails to provide this notification is liable for damages and enhanced penalties.

This report, "Information Exposed: Historical Examination of Data Breaches in New York State," analyzes the data breach notices my office has received for the last eight (8) years. It reveals that the number of reported data security breaches in New York more than tripled between 2006 and 2013. As a result, in just eight years, the number of victims in New York has exploded. Over 22 million personal records have been exposed since 2006, jeopardizing the financial health and well-being of countless New Yorkers and costing the public and private sectors in New York — and around the world — billions of dollars. This report offers fresh statistics and analysis of the scope, complexity, and cost of data breaches in New York State.

As information increasingly drives commerce and government, the challenges presented by data security breaches will continue to grow. There may be no foolproof defense against certain threats, like hacking attacks by sophisticated thieves. However, organizations can do more to prevent other types of breaches, such as insider wrongdoing and inadvertent disclosures, by ensuring that they have the best data security practices in place. This report provides recommendations that individuals and organizations can implement to protect themselves from data loss.

While the defensive measures we recommend for individuals and businesses can be helpful, the scope of the data breach problem detailed in this report demands a systemic response. Moving forward, my office plans to take a collaborative approach to address the complex problems surrounding data security. By engaging industry stakeholders and security experts, as well as lawmakers, we can ensure that organizations across the state have access to the tools and information necessary to promote the best data security practices. By doing so, we can continue to enjoy the many benefits of technological innovation without putting ourselves at risk.

Sincerely,

A handwritten signature in black ink, appearing to read "Eric Schneiderman". The signature is fluid and cursive, with a long horizontal stroke at the end.

Eric T. Schneiderman
Attorney General

KEY FINDINGS

Businesses, charitable organizations, and public agencies routinely collect personal information from New Yorkers, including Social Security and credit card numbers. The New York State Office of Attorney General (NYAG) has received notifications of organizations experiencing data breaches since the New York State Information Security Breach & Notification Act took effect in 2005. This report summarizes, analyzes, and provides context to the broader trends revealed by eight years of New York State security breach data.

Data Breaches Are An Increasing Menace

Nearly 5,000 individual data breaches were reported to the NYAG by businesses, nonprofits, and government entities between 2006 and 2013. Together, these breaches exposed 22.8 million personal records of New Yorkers. The number of data security breaches reported annually to the NYAG more than tripled between 2006 and 2013 – and 2013 was a record-setting year, during which 7.3 million records of New Yorkers were exposed. So-called mega-breaches are also becoming increasingly common: Five of the ten largest breaches reported to the NYAG have occurred since 2011.

Value Of Information & Negligence Drive Data Breaches

The overall cost of data security breaches is nothing short of staggering: In 2013 alone, breaches are estimated to have cost organizations doing business in New York State over \$1.37 billion. Hacking intrusions – in which third parties gain unauthorized access to data stored on a computer system – were the leading cause of data security breaches among organizations conducting business in New York State, accounting for roughly 40 percent of all breaches between 2006 and 2013. Hacking attacks are driven primarily by the black-market value of personal information, which can fetch up to \$45 per record. Reports of insider wrongdoing and inadvertent exposure have increased over the past eight years, with incidents of insider wrongdoing reaching their highest level in 2013. Although instances of lost or stolen equipment/documentation declined in recent years, these incidents are responsible for a significant portion of data breaches and personal record loss since 2006.

Reduce Risk By Taking Action

Organizations and individuals can take practical steps to both prevent data security breaches and mitigate potential harm in the event of a breach. The NYAG strongly suggests that all organizations collect electronic information devise and implement a comprehensive data security plan. Individuals should take steps such as monitoring financial statements and practicing their own data-minimization techniques to protect themselves against threats.

NEW YORK STATE DATA SECURITY BREACH SUMMARY

Breaches exposed 22.8 million personal records of New Yorkers between 2006 and 2013.

The number of reported data breaches tripled between 2006 and 2013.

In 2013, data breaches cost entities conducting business in New York upward of \$1.37 billion.

Hacking attacks accounted for over 40 percent of data security breaches, between 2006 and 2013.

Five of the 10 largest breaches occurred in the past three years.

INTRODUCTION: BIG DATA POSE BIG CHALLENGES

Never before have electronic data been so integral to the operations of so many organizations across New York State. Public and private organizations alike have harnessed the power of “Big Data” to provide better services and products to consumers and constituents. Big data have become increasingly affordable. In fact, according to a recent report from the White House, the cost of creating, capturing, managing, and storing digital information has dropped to only one-sixth the cost in 2005.¹

At the same time, data security breaches became an increasing threat to our digital security. According to a January 2014 Pew Research poll, nearly one-fifth of all Americans (18 percent) reported having had personal information, such as a Social Security number, credit card or bank account information, stolen in their lifetime, an increase of seven percent since July 2013.² An even higher proportion (23 percent) reported having their e-mail or social networking accounts compromised, according to the same report.

Data security breaches are more than simply a privacy concern – they can have harmful consequences. Studies by the Javelin Strategy and Research Group³ and by LexisNexis⁴ estimated approximately one-fourth of all records lost in data security breaches are used for fraudulent purposes such as identity theft. In 2012, direct and indirect identity theft losses totaled \$24.7 billion in the United States, a figure that exceeded the losses in all other categories of property crime combined.⁵

Since December 2005, the NYAG has collected information reported to the Office under the New York State Information Security and Breach Notification Act. The information in those notices, and the trends and patterns that emerged over eight years of analysis, paint a sobering picture of the state of data security in New York.

NEW YORK STATE INFORMATION SECURITY BREACH AND NOTIFICATION ACT

Effective December 7, 2005 as Business Law 899-aa

The Information Security Breach and Notification Act (Business Law 899-aa) ensures New York State residents’ right to know when a security breach has exposed their personal information. A more detailed summary and the full-text of New York State Business Law 899-aa is located in Appendix C.

KEY TERMINOLOGY

Data Security Breach (“Breach”):

An unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information. A breach can expose anywhere from a handful to millions of records.

Personal Information:

Information that can be used to distinguish or trace an individual’s identity. Personal information includes name, Social Security number, biometric records, date and place of birth, mother’s maiden name, driver’s license number, or financial account information.

Personal Records:

When an entity reports a data security breach to the NYAG, it is required to provide the number of New York residents believed to have been affected by the breach. An individual may have had three pieces of personal information compromised during the breach, but the organization will account that information as affecting one New Yorker. As such, the phrase “personal records” is a unitary term referencing the total personal information exposed during a given breach that is attributable to a given New Yorker.

Note: The personal records associated with the same individual may have been exposed in multiple breaches.

DATA BREACHES ARE AN INCREASING MENACE

In the days before Thanksgiving 2013, a highly coordinated hacking conglomerate based in Russia installed a piece of malicious software on Target's point-of-sale credit card processing system.⁶ By the time the national retailer became aware of the breach, the hackers had siphoned off personal information, including credit card numbers, of between 70 million and 110 million consumers nationwide.⁷

While the Target breach was widely publicized, it was only one example of the imminent threat data security breaches pose to organizations that collect, store, or disseminate sensitive personal information. While the extent of the Target breach was certainly alarming, the size and mission of an organization do not necessarily predict the likelihood of a breach. In fact, during the eight-year period analyzed, a widely diverse set of organizations, ranging from local family businesses to large multinational corporations, reported data security breaches to the NYAG. The trend is clear: Data security is a serious challenge for organizations of all kinds.

2013: A RECORD-SETTING YEAR FOR DATA SECURITY BREACHES IN NEW YORK

More than 900 data security breaches exposed the personal records of 7.3 million New Yorkers in 2013. This record-setting data loss was driven largely by two retail mega-breaches (Target and Living Social) that have led some to dub 2013 "The Year of the Retailer Breach."⁸ Though hacking incidents cause fewer than half of the total breaches in New York, they accounted for 96.4 percent of the total personal record loss in 2013. Hacking was not the only data security breach category to reach record highs – 2013 was also a record year for insider wrongdoing and inadvertent data disclosure events.

Data Breaches Grew in Frequency and Scope

Data breaches compromised 22.8 million personal records of New Yorkers between 2006 and 2013. More than 3,000 businesses, nonprofits, and government entities reported a data security breach to the NYAG during that eight-year period, totaling nearly 5,000 breaches. As shown in Figure 1 on the next page, hacking was the leading cause of data security breaches, accounting for roughly 40 percent of all breaches, followed by lost or stolen equipment/information (24%), and insider wrongdoing (10%).

Figure 1: Hacking Was Leading Data Breach Category in New York State

Data Security Breach Cause	Number of Breaches (% of Total)	Personal Records Exposed (% of Total)
Hacking	2,009 (40.78%)	14,416,488 (63.3%)
Lost or Stolen Equipment/Documentation	1167 (23.69%)	6,032,389 (26.51%)
Insider Wrongdoing	511 (10.37%)	1,229,779 (5.40%)
Inadvertent	997 (20.24%)	912,547 (4.01%)
Recovery By Law Enforcement ⁱ	80 (1.62%)	65,974 (0.29%)
Other	26 (0.53%)	29,609 (0.13%)
Website Compromise	53 (1.08%)	22,460 (0.10%)
Third Party Unauthorized Access	14 (0.28%)	14,500 (0.06%)
Unknown	32 (0.65%)	14,470 (0.06%)
Misplacement/Misdirection	19 (0.39%)	13,248 (0.06%)
Skimming	18 (0.37%)	1,190 (0.01%)
Total	4,926	22,752,654

Source: New York State Security Breach Reporting Forms (2006-2013)

UNDERREPORTED BREACHES: HEARTLAND PAYMENT SYSTEMS & TJX COMPANIES

While the number of personal records exposed during the eight-year period is startling in its own right, underreporting suggests the total sum of compromised records was likely much higher. For approximately six months between 2008 and 2009, a team of Russian hackers penetrated Heartland Payment Systems, one of the country's largest credit card processing systems. By the time the breach was discovered, an estimated 130 million credit card records were stolen across North America.⁹ However, when Heartland Payment Systems reported the breach to New York State, it could not provide an accurate estimate of personal record loss. As a result, the number of personal records of New Yorkers compromised as a result of this breach is not fully enumerated in the breach logs.ⁱⁱ An almost identical situation occurred in 2007, when TJX Companies (owner of T.J. Maxx, Marshalls, and Bob's Stores) experienced a massive data security breach.ⁱⁱⁱ In filings to the Securities and Exchange Commission, TJX Companies indicated that credit card information for 45.6 million Americans had been stolen during the breach,¹⁰ but they also could not provide an accurate number or estimate of personal record exposure.

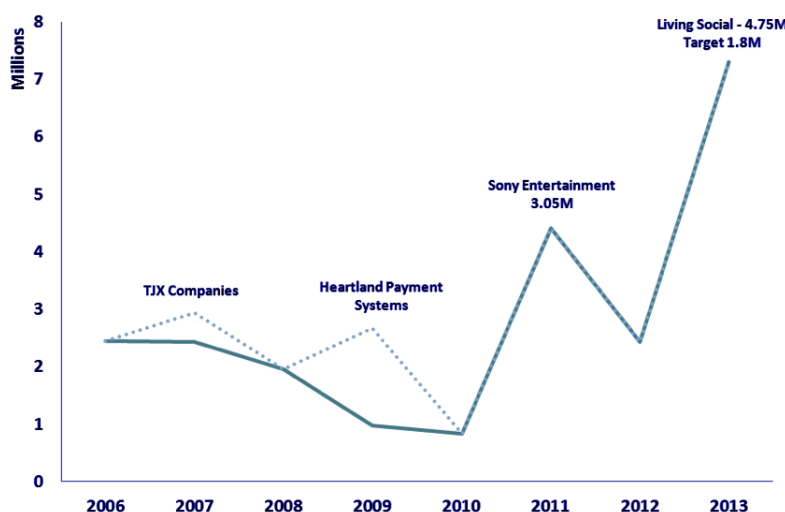
ⁱ This category refers exclusively to notifications made by American Express to New York State. When law enforcement agencies report fraudulent activity of New Yorkers' accounts to American Express, they also report it to the NYAG

ⁱⁱ Although Heartland Payment Systems did not report a number of personal record exposures to the NYAG, five independent entities that used Heartland's services made notifications to the NYAG in 2009, totaling 13,463 personal records of New Yorkers

ⁱⁱⁱ Although TJX Companies did not report a number of personal record exposures to the NYAG, independent entities made notifications of information loss due to the breach, totaling 12,086 personal records of New Yorkers

The annual number of data security breach occurrences reported to the NYAG has more than tripled since 2006, with increases almost every year. Over half the total data security breaches reported to the NYAG have occurred in just the past three years. Figure 2, below, charts the number of personal records exposed each year between 2006 and 2013. The solid series depicts the number of personal records exposed that were reported to the NYAG. Considering the magnitude of the TJX Companies and Heartland Payment System breaches, the second “dotted” series adds a conservative estimate of the potential number of personal records exposed by both the TJX Companies and Heartland Payment Systems breaches.^{iv}

Figure 2: Number of Personal Records Exposed Volatile but Trending Upward



Source: New York State Security Breach Reporting Forms (2006-2013)

Mega-breaches: Large-Scale Events Drive Data Loss

In just eight years, 28 mega-breaches^v were reported to the NYAG, exposing approximately 18.2 million personal records of New Yorkers. Despite constituting only a sliver of reported breach events between 2006 and 2013, these 28 mega-breaches were responsible for nearly 80 percent of personal records exposed. What’s more, mega-breaches are a growing phenomenon – five of the 10 largest breaches reported to the NYAG occurred in the past three years. Figure 3, on the next page, lists the top 10 breaches since 2006 in terms of numbers of personal record exposures. Also shown below, reports of hacking intrusions and lost or stolen equipment are the two primary drivers of mega-breaches. Hacking, detailed in the next section, poses a particularly nefarious challenge to data security, as large volumes of sensitive information are typically obtained for the express purpose of committing fraud.

^{iv} The NYAG estimated the number of New Yorkers affected by the Heartland Payment Systems and TJX Companies breaches using the 2013 Target breach as a rough benchmark. While more records were exposed during the Heartland Payment Systems breach than in the Target breach, the NYAG conservatively estimated the Heartland breach to have affected at least 1.7 million New Yorkers. With TJX Companies, where approximately 1/3 of the number of personal records were exposed, the NYAG conservatively estimated that at least 500,000 New Yorkers were affected by the TJX Companies breach.

^v Data breach events during which the personal records of at least 100,000 New Yorkers were compromised.

Figure 3. Five of Ten Largest Breaches Occurred Since 2011

Reporting Entity	Year	Personal Records Exposed	Cause of Breach
LivingSocial	2013	4,750,000	Hacking
Sony Entertainment	2011	3,050,000	Hacking
Target Corporation	2013	1,797,000	Hacking
Heartland Payment Systems	2008-09	1,700,000	Hacking
NYS Electric & Gas	2012	1,699,905	Hacking
BNY Mellon Bank	2008	1,602,567	Lost/Stolen Hardware/Documentation
CS STARS	2006	722,000	Lost/Stolen Hardware/Documentation
North Bronx Healthcare	2011	595,509	Lost/Stolen Hardware/Documentation
TJX Companies	2007	500,000	Hacking
TD Ameritrade Holding Corp	2007	486,738	Hacking

Source: New York State Security Breach Reporting Forms (2006-2013)

Retailers and Health Care Providers Are Particularly Vulnerable to Data Security Breaches

Certain industries were particularly susceptible to data security breaches during the eight years analyzed. Since 2006, a total of 241 institutions (approximately 8 percent of all reporting entities) reported three or more data security breaches to the NYAG. As shown below in Figure 4, retailers are the most likely to experience three or more data breaches. This is largely because retailers' payment systems (particularly restaurant payment systems) have become a favorite target of hackers.¹¹ Data breaches in the health care industry have exposed the largest number of personal records of New Yorkers since 2006. As the health care industry moves toward increasing digitization, it has become a repository for large troves of sensitive information, making the industry uniquely susceptible to data loss, particularly through lost or stolen electronic storage equipment.

Figure 4: Retail Services Are Most Likely to Be “Multiple Breach Entities”

Industry Type	Entities With 3+ Breaches	Personal Records Exposed
Retail Services	54	163,319
Financial Services	31	624,000
Health Care	29	1,012,269
Banking	27	560,208
Insurance	20	72,138
Professional Services	16	788,280
Educational Inst.	15	103,787
Government Agency	14	86,548
Loan Services	9	133,866
Hospitality	8	16,091
Technology	7	13,195
Telecommunications	4	80,963
Credit Reporting	3	3,120
Credit Card Company	2	237,296
Nonprofit	1	507
Public Utility	1	50,456
Grand Total	241	3,946,043

Source: New York State Security Breach Reporting Forms (2006-2013)

VALUE OF INFORMATION& NEGLIGENCE DRIVE DATA BREACHES

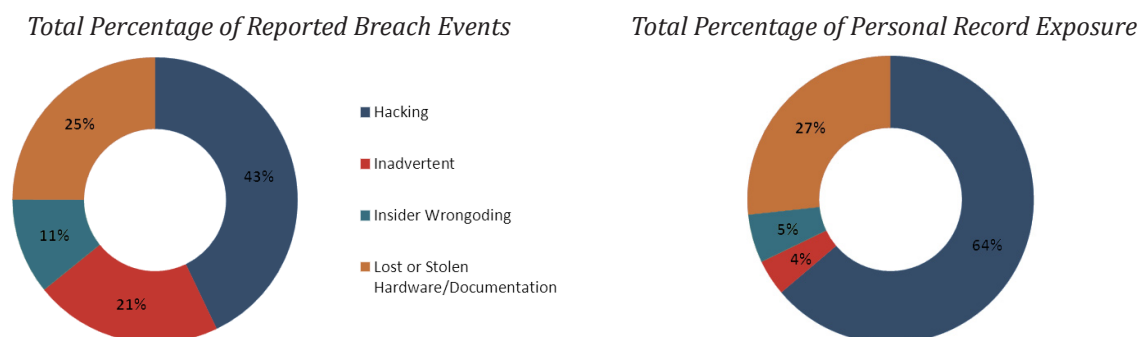
The personal information that makes up personal records is a valuable commodity on the digital black market. Freshly acquired stolen credit card numbers can fetch up to \$45 per record, while other types of personal information, such as Social Security numbers and online account information, can command even higher prices.¹² Nonfinancial information can be more valuable, as fraudulent use of this data is more difficult to detect and the information can be used for a broader range of purposes.¹³ For example, a stolen Facebook account can provide an access point to a wide range of user accounts (many people use the same password across multiple online platforms), or can be used as a vehicle to steal information (i.e. through phishing – sending links that provide hackers with access to a computer) from others within that individual's social network.¹⁴ For criminals, stealing data can be as lucrative as drug trafficking, but with far less risk and fewer barriers to entry.¹⁵ This combination of high profit potential and low risk drives the market for hacking breaches.

Not all data security breaches are created equal. For example, the causes of an accidental breach can range from a simple mistake to broad negligence, while a hacking attack can originate with a single disgruntled employee with limited technical proficiency, or a highly sophisticated international hacking syndicate. Consequently, breach events can vary widely in terms of scope and scale. For instance, incidents of inadvertent exposure, such as a small business accidentally faxing a document to a subcontractor without redacting a customer's name and credit card number, tend to expose fewer personal records despite occurring relatively frequently. Hacking attacks, which are often undertaken with the explicit goal of stealing information, tend to compromise many more personal records of New Yorkers.

The Big Four

Four data breach categories accounted for almost all breaches in New York State. The four primary categories of data breaches are: hacking, inadvertent exposure, insider wrongdoing, and lost or stolen equipment/documentation. These four categories accounted for 95 percent of the total breach events reported to the NYAG and over 99 percent of total personal record loss between 2006 and 2013. Figure 5, below, depicts the percentage of breach events, and the percentage of personal records exposed by those events, that were attributable to each of those four categories.

**Figure 5: Most Data Breaches Attributable to Four Types;
Some Categories Inflict Greater Record Loss**



Source: New York State Security Breach Reporting Forms (2006-2013)

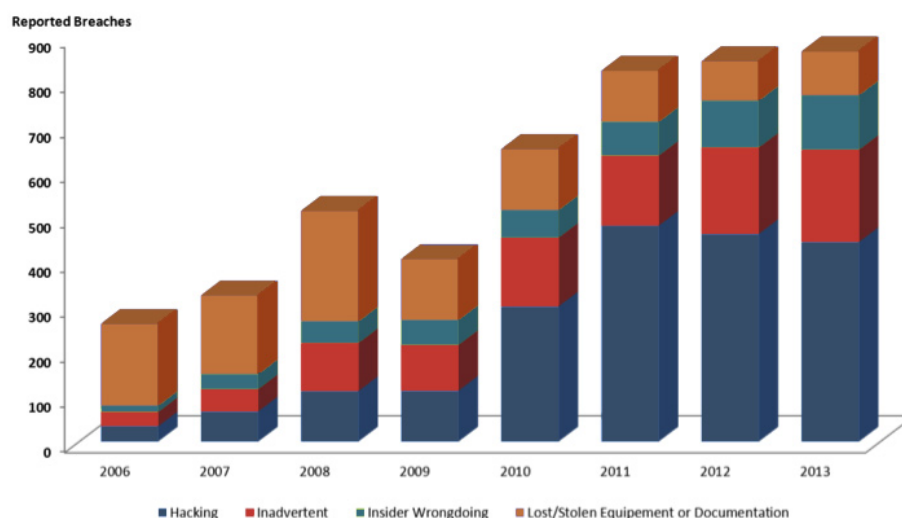
NEW TECHNOLOGY, NEW THREATS

The rapid pace of innovation — particularly in mobile technology — will continue to provide additional platforms for hackers to exploit. Countless Americans store huge amounts of personal information on their mobile devices, and malware created to exploit mobile software platforms has started to proliferate.¹⁶ Additionally, mobile phone users often connect to unsecured and unencrypted public WiFi networks that can be easily penetrated by an experienced hacker.¹⁷ Americans seem largely unaware of these threats, as they increasingly use mobile devices to conduct sensitive transactions, such as mobile banking, despite the fact that many of those activities have proven vulnerable to hacking attacks.¹⁸

Value of Information Incentivizes Hacking and Insider Wrongdoing

The number of hacking incidents reported to the NYAG showed the most dramatic increase over the eight-year period analyzed. A mere 34 instances of hacking were reported to the NYAG in 2006; those grew to over 400 reported incidents in every year since 2011, increasing most dramatically between 2009 and 2011. During that period, easy-to-use “crimeware”¹⁹ applications such as “ZeuS” source code became widely available, according a 2014 RAND Corporation report on Cybercrime Tools and Stolen Data.²⁰ After the original code for “ZeuS” was published publicly, thousands of variations were created, allowing the program to flourish and largely evade eradication. To date, “ZeuS” and its primary offshoot, “Citadel,” remain a hacker favorite for stealing information.²¹ Figure 6, below, illustrates the larger trends in the top four categories of breaches between 2006 and 2013. Reports of insider wrongdoing and inadvertent exposure have increased steadily over the past eight years as well, with incidents of insider wrongdoing reaching their highest level in 2013.

Figure 6: Hacking Grows to Dominate Reported Data Security Breach Types

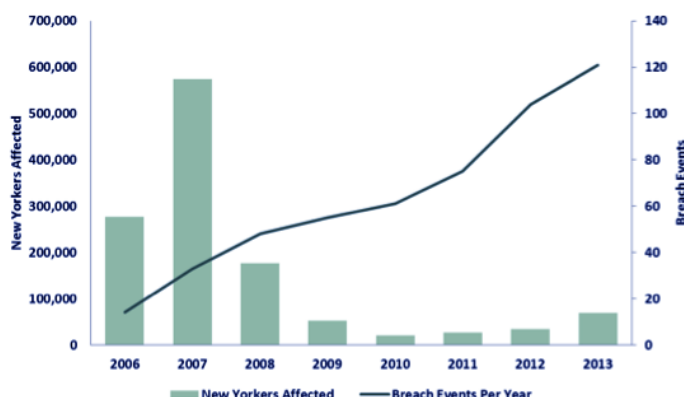


Source: New York State Security Breach Reporting Forms (2006-2013)

Despite increased awareness and prevention efforts, hacking events are likely to continue their meteoric rise. Hackers and the black markets where they exchange tools and information are becoming increasingly sophisticated and specialized.²² In fact, some security experts believe that hackers actually coordinate to stagger large-scale breach events in order to preserve the scarcity of stolen information, thereby inflating prices for stolen data.²³

Threats to data security are not always external — instances of insider wrongdoing grew to an all-time high in 2013. Like hacking, insider wrongdoing presents a unique but important challenge to data security, as compromised personal records are often obtained exclusively for fraudulent purposes. As shown in Figure 7 below, instances of insider wrongdoing have steadily increased since 2006 and reached a record high of 121 reported instances in 2013. However, with the exception of 2007, the volume of personal records exposed generally decreased during that time. In 2007, there was a jump in the number of personal records belonging to New Yorkers that were exposed, mainly due to a single event – the Certegy Check Services breach, which accounted for approximately 80 percent (470,696) of New Yorkers’ records affected that year.

Figure 7: Insider Wrongdoing Rises But Exposes Fewer Personal Records Since 2006



Source: New York State Security Breach Reporting Forms (2006-2013)

WHO MONITORS THE MONITORS?

CERTEGY CHECK SERVICES EXPOSES 470,696 PERSONAL RECORDS

Despite making up only a small portion of insider wrongdoing breach events, credit reporting services exposed more New Yorkers’ personal records than any other industry. This fact is troubling, considering that companies are typically encouraged to provide credit monitoring services to customers following a breach event. The Certegy Check Services data security breach event is one particularly nefarious example. Certegy Check Services is a consumer reporting agency that helps retailers determine whether to accept a personal check from consumers at checkout. In 2007, a database analyst stole the personal information of approximately 8.5 million individuals and sold the information to advertising list broker JAM Marketing, which in turn sold the information to a variety of direct marketing firms.²⁴ Certegy Check Services ultimately paid fines and provided credit monitoring services for those affected by the breach. The database analyst is currently serving 57 months in federal prison for fraud.²⁵ JAM Marketing, which claimed it was unaware that the information had been stolen, escaped penalty for the breach.

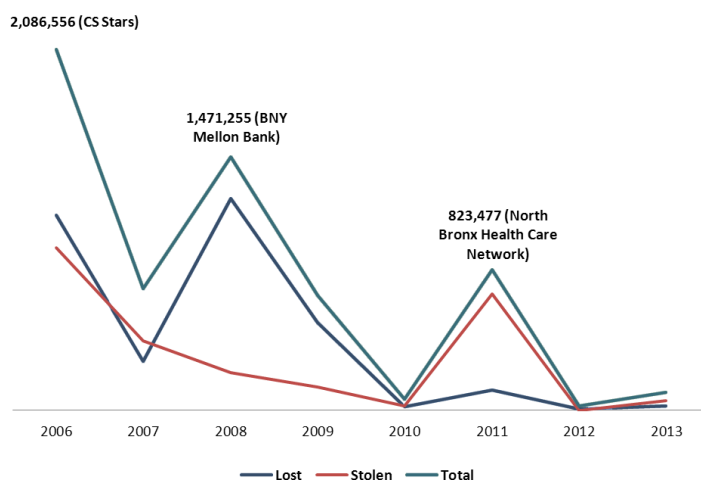
Information Also Exposed Through Preventable Circumstances

The theft or loss of equipment or documentation containing personal information accounted for almost a quarter of total breach events. Laptops and mobile devices can be stolen solely for the value of the electronic equipment, and lost equipment does not always fall into the wrong hands. Reports of stolen/lost equipment peaked at the height of the recession in 2008 and gradually declined before experiencing a recent uptick. Whether personal records were actually disclosed during these events is often unclear. The amount of personal record exposure caused by these types of breaches has been volatile, largely because of a few large events. For example, the spike in 2008, shown in Figure 8 below, is largely attributable to the loss of BNY Mellon's back-up tapes, which exposed 1.2 million personal records of New Yorkers. Overall, the volume of personal records exposed by lost or stolen equipment and documents declined significantly since 2006.

"LOST" VS. "STOLEN" HARDWARE/DOCUMENTATION: BNY MELLON AND NORTH BRONX HEALTH CARE NETWORK (NBHCN)

The BNY Mellon and NBHCN incidents are two large breaches that illustrate the thin line between hardware/information being reported as "stolen" or "lost." In both instances, tape drive storage devices (i.e. "back-up tapes") that were being transported to a storage facility by a third party delivery service disappeared in transit. However, BNY Mellon reported that one tape was "lost," while NBHCN noted that its tapes had been left unattended in an unlocked vehicle for a short duration and were therefore "stolen." In both events, large amounts of highly sensitive and personal information were put at risk, including Social Security numbers, bank account information, and health records.

**Figure 8: Lost and Stolen Information/Documentation Declining;
Two Events Cause Spikes**



Source: New York State Security Breach Reporting Forms (2006-2013)

DATA BREACHES HAVE BILLION-DOLLAR CONSEQUENCES

Data security breaches have significant financial consequences, particularly for the organizations involved. According to a report published by Symantec and the Ponemon Institute in 2013,²⁶ each personal record compromised during a data breach costs an entity approximately \$188. By that estimate, based on NYAG data, breaches cost organizations doing business in New York State over \$1.37 billion in 2013 alone.^{vi}

Why are the breaches so costly to organizations? After a data breach is discovered, organizations expend significant resources investigating the incident, rectifying security lapses, and notifying those affected, including providing written notice, staffing help centers, and providing free credit monitoring services for affected customers. In certain instances, the organization may also incur sizable legal fees from litigation surrounding the breach. There are also indirect economic consequences associated with a breach. After major breaches that affected millions of customers, both Sony Entertainment and Target experienced a crisis in both consumer and investor confidence. In the year following its 2013 breach, the Target Corporation reported a 46 percent decrease in net earnings and experienced a similarly sharp decrease in stock price.²⁷ Sony Entertainment experienced a 6 percent stock price decrease and incurred estimated revenue losses of more than \$1 billion²⁸ after approximately 77 million accounts were stolen from its PlayStation Network during a hacking attack in 2011.²⁹

Quantifying costs for individual victims of data breaches is more complicated, as not every breach will result directly in financial loss. According to LexisNexis' "True Cost of Fraud" report, approximately 25 percent of victims of data breaches subsequently suffer identity theft.³⁰ While the Bureau of Justice Statistics found that only 14 percent of those victimized by the identity theft incur out-of-pocket costs,³¹ this statistic likely obscures the true costs of identity theft. For example, approximately 30 percent of individuals who experienced the misuse of personal information for fraudulent purposes spent over a month clearing up associated financial and credit problems.³²

^{vi} Calculation: \$188 per record x 7,300,222 records exposed = \$1,372,441,736.

REDUCE RISK BY TAKING ACTION

Despite the risks posed by data security breaches, individuals and organizations can take practical steps to better protect themselves against threats. While it may be impossible to completely prevent data loss, organizations that implement data security plans can greatly reduce the harm caused by a data security breach. The need for a comprehensive data security plan is not limited to large corporations or those who deal heavily in data. A survey conducted by the Ponemon Institute in 2013 indicated that more than half of U.S. small businesses have experienced at least one data breach.³³ Individuals can also take steps to protect themselves from a breach, and safeguard their personal and financial information if they are the victim of a breach.

Steps For Organizations To Protect Themselves

The NYAG encourages businesses to adopt sound data security practices for all levels of data. When combined with other publicly available data, even seemingly innocuous information can identify individuals and leave them susceptible to identity theft or financial fraud. Sensitive personal information including email addresses, phone numbers, and zip codes, should be protected under the same guidelines as highly sensitive information such as Social Security numbers, credit card numbers, and physical addresses.

The NYAG recommends following these five simple steps to help protect sensitive personal information against unauthorized disclosures.

1. Understand Where Your Business Stands

The first step toward effective data security is to understand what information your business requires for its operation, what data have already been collected and stored, how long the data are needed, and what steps have been taken to ensure security. Organizations should review how sensitive information is acquired, how it is shared with third parties, and what access controls are in place.

2. Identify and Minimize Data Collection Practices

Put simply, data that do not exist cannot be stolen or lost. Collect only information that you need, store it only for the minimum time that you need it, and deploy data minimization tactics wherever possible. For example, if your company uses a point-of-sale system, ensure that expiration dates are not stored with credit card numbers. Reduce the use of highly sensitive data points, such as Social Security numbers, unless absolutely necessary, and minimize the length of retention for such data. Delete any information you no longer need.

3. Create an Information Security Plan That Includes Encryption

Creating a comprehensive Information Security Plan is a complex but necessary endeavor. Studies show that entities with an effective plan will not only articulate technical standards but will also incorporate training, awareness, and detailed procedural steps in the event of data breaches. The plan should:

- Require a privacy policy that reflects the unique business practices and organizational features of the company or organization. The policy should

use clear language and be made conspicuously available to customers and employees.

- Incorporate procedures restricting access to records and files containing personal information to employees for whom access is essential for their job function. Assign a unique identifier to each employee who has access to the system and require passwords that are reasonably designed to maintain system integrity.
- Frequently monitor systems for unauthorized use or access.
- Implement effective technical safeguards for sensitive personal information:
 - Require encryption of all stored sensitive personal information – including on databases, hard drives, laptops, and portable devices.
 - Minimize storage of sensitive personal information on devices connected to the Internet.
 - Implement hashing and salting of stored user passwords.^{vii}
 - Incorporate firewalls and up-to-date security software to protect corporate networks.
 - Ensure that all devices issued to employees require secure authentication to access encrypted sensitive personal information.
- Implement education and training programs for employees on the proper use of computer systems, including accessing and transferring data, and regarding cybersecurity threats such as phishing.
- Implement information disposal practices that are reasonable and appropriate to prevent unauthorized access to and use of personal information. The traditional “delete” function on a computer is usually not sufficient because a file may continue to exist on a hard drive. A better practice is to use software such as a wipe utility program to permanently erase data from a hard drive, scanners, and other devices.
- Establish an oversight committee or chief data security officer position to ensure implementation and adoption of the plan and periodic review.
- Annually review your organization’s data practices for compliance with state and federal laws, such as the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act and various state data security and notification laws.

4. Implement Information Security Plan

Successful implementation of a thoughtfully designed plan can be one of the most effective ways to minimize the risk of a data breach. Elements to consider when implementing a plan include:

- Ensuring employees are trained and aware of the plan.
- Ensuring third parties with whom you might share data are aware of your plan and the procedures it entails.
- Conducting regular audits to ensure compliance with the plan.

^{vii} “Hashing” turns passwords into a “fingerprint,” allowing the storage of passwords that cannot be read or translated back. It also allows the company to verify that a user’s password is correct. “Salting” makes password hashing more secure by adding a random string of characters to passwords before their hash is calculated, which makes them harder to crack.

- Conducting regular reviews of the provisions of the plan to ensure it continues to conform with evolving industry best practices.

Remember to investigate all security incidents immediately and thoroughly. In the event of a breach, the law may require you to notify consumers, law enforcement, state Attorney Generals' offices, credit bureaus, and other businesses.

5. Offer Mitigation Products in the Event of a Breach

While not required by law, New Yorkers affected by a data breach should be provided with mitigation services for free. These include credit monitoring, which provides alerts, usually by email, whenever an application for new credit is submitted to a consumer credit reporting agency, and a security freeze, which blocks new credit accounts. This is especially necessary in breaches that compromise a person's Social Security number or driver's license number, as it allows "new account" fraud — one of the most harmful types of identity theft. The cost of clearing up "new account" identity theft can easily reach into the thousands of dollars and require hundreds of hours attending to administrative burdens.

Steps For Individuals To Protect Themselves

The NYAG suggests that consumers guard against threats in the following ways:

- Create strong passwords for online accounts and update them frequently. Use different passwords for different accounts, especially for websites where you have disseminated sensitive information, such as credit card or Social Security numbers.
- Carefully monitor credit card and debit card statements each month. If you find any abnormal transactions, contact your bank or credit card agency immediately.
- If possible, do not write down or store passwords electronically. If you do, be extremely careful of where you store passwords. Be aware that any passwords stored electronically (such as in a word processing document or cell phone's notepad) can be easily stolen and provide fraudsters with one-stop shopping for all your sensitive information. If you hand-write passwords, do not store them in plain sight.
- Do not post any sensitive information on social media. Information such as birthdays, addresses, and phone numbers can be used by fraudsters to authenticate account information. Practice data minimization techniques. Don't overshare!
- Always be aware of the current threat landscape. Stay up to date on media reports of data security breaches and consumer advisories.

Those who believe they have been victimized by a data security breach must take action. However, the appropriate action will vary depending on the nature of the breach.

1. User Names and Passwords

For user names and passwords, change them immediately on the relevant account, and monitor the account for unusual activity. If you use the same user name or password on other accounts, change those as well.

2. Credit Card Numbers

For breaches involving credit card numbers, Social Security numbers and other sensitive numbers, create an Identity Theft Report by filing a complaint with the Federal Trade Commission and printing your Identity Theft Affidavit. You can call the

Federal Trade Commission (FTC) at 1-877-438-4338 or complete the form online at: <http://bit.ly/NYAGDATA>. Use the Identity Theft Affidavit to file a police report and create your Identity Theft Report. An Identity Theft Report will help you deal with credit reporting companies, debt collectors, and any fraudulent accounts that the identity thief opened in your name. You may also want to put a fraud alert (a red flag that signals to credit grantors that you may have been a victim of suspicious activity) and/or a security freeze (which prevents your credit file from being reported to third parties) on your credit report by notifying each of the credit reporting agencies (Equifax, TransUnion, or Experian). A security freeze remains on your credit file until you remove it or lift it temporarily when applying for credit services.

**CREDIT AGENCY
CONTACT
INFORMATION**

Equifax
1-800-525-6285

Experian
1-888-397-3742

TransUnion
1-800-680-7289

APPENDIX A: METHODOLOGY

Data security breaches between 2005 and 2009 were recorded in Microsoft Word documents, while 2010-2014 breaches were recorded using Microsoft Excel Spreadsheets. After the data were successfully combined into one spreadsheet, a significant amount of “cleaning” was necessary to correct inconsistencies that prevented accurate analysis.

This process also included standardizing breach events into broader categories for analysis, since some notice descriptions were often brief and/or ambiguous. Despite best efforts, some descriptions were simply too ambiguous, and were therefore categorized as “other.” Examples of these descriptions include other criminal acts (“extortion,” “mail tampering,” and “check counterfeiting”) and the unexplainable (“files found outdoors” and “student chose user PIN of another”). Breach events that were recorded without any discernable descriptions were categorized as “unknown.”

The construction of the “hacking” category included descriptions such as “computer virus” or “malware,” as well as “unauthorized intrusion” or “unauthorized access.” Based simply on those descriptions, some of the unauthorized access/intrusion categories could have been misclassified.

APPENDIX B: WHAT'S NOT REPORTED

This report is an analysis of the data breach notification reports received by the NYAG over the course of many years, as required by state law. Under New York State law, notification is required only if personally identifying information like a name, in addition to a protected number, like a credit card or Social Security number, is disclosed. Thus, this report does not include any information about the thousands of data breaches that involved disclosure of other sensitive information but did not require notification under law.

For example, in 2011, hackers gained access to data from online shoe and clothing retailer Zappos, owned by Amazon.com. Over 24 million customers' personal details and account information were stolen, including names, email addresses, billing and shipping addresses, the last four digits of credit card numbers, and "cryptographically scrambled" versions of website passwords. The information accessed did not evoke New York's data breach notification laws because it did not include the customers' full credit card or Social Security numbers. Thus, Zappos did not submit a data breach notification form to the NYAG, and the details of this breach are not provided in this report. Zappos did, however, provide direct notice to its customers, including New York residents.

This report also does not provide any information on total consumer losses from data breaches. This information is not required to be disclosed during the notification process and would be collected only if the NYAG conducted a follow-up investigation.

APPENDIX C: NEW YORK DATA SECURITY BREACH NOTIFICATION LAW

In late 2005, New York State Business Law was amended by adding Article 39F Section 899-aa,³⁴ requiring any person or commercial entity conducting business in New York State, who owns, licenses, maintains, or disseminates as a third party computerized data that includes private information to disclose all breaches of the security of the computerized data system containing private information to the State Police, Department of Consumer Protection, and the Office of the Attorney General. A similar provision, State Technology Law §208, requires state governmental entities to make the same notifications.³⁵ Breach notification must be made as quickly as possible and without unreasonable delay, consistent with the needs of law enforcement or measures necessary to determine the scope of the breach and/or restore reasonable integrity to the system.

The law also stipulates that entities have a “notification obligation” to any New Yorker whose private information was acquired (or reasonably believed to have been acquired) during the breach. Notification can be made either by mail or phone (email with consent), or if larger in scale (costing over \$250,000 to make the notifications), through conspicuous notice such as through the entity’s website or via notification of major media outlets. If more than 5,000 New Yorkers were affected, the entity is also required to notify the credit reporting agencies (Equifax, Experian, and TransUnion) as to the timing, content, and distribution of the notices and the approximate number of New Yorkers affected. The Attorney General may bring action if any of the aforementioned articles are not satisfied by the breached entity, and the court may impose fines ranging from \$10 to \$150,000.

Information for the log is gleaned from the New York State Security Breach Reporting Form, available in PDF form on the NYAG’s website. A copy of this form is shown in Appendix D of this report. Entities are also required to submit a copy of the correspondence sent to individuals affected by the breach – from which, at times, additional information is garnered for the logs.

[General Business Law §899-aa.](#)

Notification; person without valid authorization has acquired private information.

1. As used in this section, the following terms shall have the following meanings:

(a) “Personal information” shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person;

(b) “Private information” shall mean personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired:

(1) Social Security number;

(2) driver’s license number or non-driver identification card number;

or

(3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account;

“Private information” does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.

(c) “Breach of the security of the system” shall mean unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business. Good-faith acquisition of personal information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the following factors, among others:

(1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or

(2) indications that the information has been downloaded or copied; or

(3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

(d) “Consumer reporting agency” shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state Attorney General and furnished upon request to any person or business required to make a notification under subdivision two of this section.

2. Any person or business which conducts business in New York State, and which owns or licenses computerized data which includes private information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York State whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

3. Any person or business which maintains computerized data which

includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

4. The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation.

5. The notice required by this section shall be directly provided to the affected persons by one of the following methods:

- (a) written notice;
- (b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction.
- (c) telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons; or
- (d) Substitute notice, if a business demonstrates to the state attorney general that the cost of providing notice would exceed \$250,000, or that the affected class of subject persons to be notified exceeds \$500,000, or such business does not have sufficient contact information. Substitute notice shall consist of all of the following:
 - (1) e-mail notice when such business has an e-mail address for the subject persons;
 - (2) conspicuous posting of the notice on such business's web site page, if such business maintains one; and
 - (3) notification to major statewide media.

6. (a) whenever the attorney general shall believe from evidence satisfactory to him that there is a violation of this article, he may bring an action in the name and on behalf of the people of the State of New York, in a court of justice having jurisdiction to issue an injunction, to enjoin and restrain the continuation of such violation. In such action, preliminary relief may be granted under article sixty-three of the civil practice law and rules. In such action, the court may award damages for actual costs or losses incurred by a person entitled to notice pursuant to this article, if notification was not provided to such person pursuant to this article, including

consequential financial losses. Whenever the court shall determine in such action that a person or business violated this article knowingly or recklessly, the court may impose a civil penalty of the greater of \$5,000 or up to \$10 per instance of failed

notification, provided that the latter amount shall not exceed \$150,000.

(b) the remedies provided by this section shall be in addition to any other lawful remedy available.

(c) no action may be brought under the provisions of this section unless such action is commenced within two years immediately after the date of the act complained of or the date of discovery of such act.

7. Regardless of the method by which notice is provided, such notice shall include contact information for the person or business making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.

8. (a) In the event that any New York residents are to be notified, the person or business shall notify the state Attorney General, the Department of State and the Division of State Police as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

(b) In the event that more than five thousand New York residents are to be notified at one time, the person or business shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

9. The provisions of this section shall be exclusive and shall preempt any provisions of local law, ordinance or code, and no locality shall impose requirements that are inconsistent with or more restrictive than those set forth in this section.

APPENDIX D: NEW YORK STATE SECURITY BREACH REPORTING FORM

NEW YORK STATE SECURITY BREACH REPORTING FORM

Pursuant to the Information Security Breach and Notification Act
(General Business Law §899-aa)

Name and address of Entity that owns or licenses the computerized data that was subject to the breach:

Street Address: _____
City: _____ State: _____ Zip Code: _____

Submitted by: _____ Title: _____ Dated: _____

Firm Name (if other than entity): _____
Telephone: _____ Email: _____
Relationship to Entity whose information was compromised: _____

Type of Organization (please select one): ☐ Governmental Entity in New York State; ☐ Other Governmental Entity;
☐ Educational; ☐ Health Care; ☐ Financial Services; ☐ Other Commercial; or ☐ Not-for-profit.

Number of Persons Affected:

Total (Including NYS residents): _____ NYS Residents: _____

If the number of NYS residents exceeds 5,000, have the consumer reporting agencies been notified? ☐ Yes ☐ No

Dates: Breach Occurred: _____ Breach Discovered: _____ Consumer Notification: _____

Description of Breach (please select all that apply):

- ☐ Loss or theft of device or media (e.g., computer, laptop, external hard drive, thumb drive, CD, tape);
☐ Internal system breach; ☐ Insider wrongdoing; ☐ External system breach (e.g., hacking);
☐ Inadvertent disclosure; ☐ Other specify: _____

Information Acquired: Name or other personal identifier in combination with (please select all that apply):

- ☐ Social Security Number
☐ Driver's license number or non-driver identification card number
☐ Financial account number or credit or debit card number, in combination with the security code, access code, password, or PIN for the account

Manner of Notification to Affected Persons - ATTACH A COPY OF THE TEMPLATE OF THE NOTICE TO AFFECTED NYS RESIDENTS:

- ☐ Written ☐ Electronic ☐ Telephone ☐ Substitute notice

List dates of any previous (within 12 months) breach notifications: _____

Identify Theft Protection Service Offered: ☐ Yes ☐ No

Duration: _____ Provider: _____
Brief Description of Service: _____

ENDNOTES

1. Podesta, John , John Holdren, Penny Pritzker, Ernest Moniz, and Jeffrey Zients, “Big Data: Seizing Opportunities, Preserving Values,” The White House, 1 May 2014, http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.
2. Madden, Mary, “More online Americans say they’ve experienced a personal data breach,” Pew Research Center, 14 April 2014, <http://www.pewresearch.org/fact-tank/2014/04/14/more-online-americans-say-theyve-experienced-a-personal-data-breach/>.
3. “2013 IDENTITY FRAUD REPORT: Data Breaches Becoming a Treasure Trove for Fraudsters,” Javelin Strategy & Research, 2013, <https://www.javelinstrategy.com/brochure/276#DownloadReport>.
4. “2013 LexisNexis True Cost of Fraud Study: Merchants Struggle Against an Onslaught of High-Cost Identity Fraud and Online Fraud,” LexisNexis, September 2013, <http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2013.pdf>.
5. Harrell, Erika, and Lynn Langton, “Victims of Identity Theft, 2012,” U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, December 2013, <http://www.bjs.gov/content/pub/pdf/vit12.pdf>.
6. Krebs, Brian, “A First Look at the Target Intrusion, Malware,” Krebs on Security, 15 January 2014, <http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/>.
7. Finkle, Jim, and Mark Hosenball, “Exclusive: More well-known U.S. retailers victims of cyber attack-sources,” Reuters, 12 January 2014, <http://www.reuters.com/article/2014/01/12/us-target-databreach-retailers-idUSBREA0B01720140112>.
8. “2014 Data Breach Investigations Report,” Verizon Enterprise Solutions, 2014, <http://www.verizonenterprise.com/DBIR/2014/>.
9. Krebs, Brian, “Heartland Payment Systems,” Krebs on Security, 2013-2014, <http://krebsonsecurity.com/tag/heartland-payment-systems/>.
10. Vijayan, Jaikumar, “TJX data breach: At 45.6M card numbers, it’s the biggest ever,” Computerworld, 29 March 2007, sec. News, http://www.computerworld.com/s/article/9014782/TJX_data_breach_At_45.6M_card_numbers_it_s_the_biggest_ever.
11. Perlroth, Nicole, “Russian Arrested in Guam on Array of U.S. Hacking Charges,” New York Times , 7 July 2014, sec. Security, http://bits.blogs.nytimes.com/2014/07/07/russian-arrested-in-guam-on-array-of-u-s-hacking-charges/?_php=true&_type=blogs&_r=0charges/?_php=true&_type=blogs&_r=0.
12. Ablon, Lillian, Martin Libicki, and Andrea Golay, “Markets for Cybercrime Tools and Stolen Data: Hackers’ Bazaar,” RAND Corporation: National Security Research Division, 2014, http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.
13. Ibid.
14. Callahan, Michael, “Why Your Twitter Account May Be More Valuable Than Your Credit Card,” Juniper Networks, 24 March 2014, <http://forums.juniper.net/t5/Security-Mobility-Now/Why-Your-Twitter-Account-May-Be-More-Valuable-Than-Your-Credit/ba-p/234270>.
15. Ablon, Lillian, Martin Libicki, and Andrea Golay, “Markets for Cybercrime Tools and Stolen Data: Hackers’ Bazaar,” RAND Corporation: National Security Research Division, 2014, http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.
16. “Mobile devices are a leading data breach threat,” Risk Management and Safety Eline, 3 April 2014, <http://www.associatedfinancialgroup.com/Data/eLineNewsletters/RiskManagement/Vol13/No4apr14/riskartApr14.asp>.
17. Kassner, Michael, “Convenience or security: You can’t have both when it comes to Wi-Fi,” TechRepublic, 24 June 2013, <http://www.techrepublic.com/blog/it-security/convenience-or-security-you-cant-have-both-when-it-comes-to-wi-fi/>.
18. Constantin, Lucian. “Security analysis of mobile banking apps reveals significant weaknesses,” Computerworld, 9 January 2014, sec. News, http://www.computerworld.com/s/article/9245298/Security_analysis_of_mobile_banking_apps_reveals_significant_weaknesses.
19. “2014 Data Breach Investigations Report,” Verizon Enterprise Solutions, 2014, <http://www.verizonenterprise.com/DBIR/2014/>.
20. Ablon, Lillian, Martin Libicki, and Andrea Golay, “Markets for Cybercrime Tools and Stolen Data: Hackers’ Bazaar,” RAND Corporation: National Security Research Division, 2014, <http://www.rand.org/content/dam/>

rand/pubs/research_reports/ RR600/RR610/RAND_RR610.pdf.

21. "2014 Data Breach Investigations Report," Verizon Enterprise Solutions, 2014, <http://www.verizonenterprise.com/DBIR/2014/>.
22. Ablon, Lillian, Martin Libicki, and Andrea Golay, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar," RAND Corporation: National Security Research Division, 2014, http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.
23. Ibid.
24. Abramovich, Giselle, "Certegy's ID breach lost 8.5 million names," Direct Marketing News, 8 August 2007, sec. Miscellaneous, <http://www.dmnews.com/certegys-id-breach-lost-85-million-names/article/98116/>.
25. McGlasson, Linda, "Certegy Reaches Data Breach Settlement," Bank Info Security, 20 April 2010, sec. Articles, <http://www.bankinfosecurity.com/certegy-reaches-data-breach-settlement-a-2441>.
26. 2013 Cost of Data Breach Study: Global Analysis," Ponemon Institute, May 2013, https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf.
27. Harris, Elizabeth, "Data Breach Hurts Profit at Target," New York Times, 26 February 2014, sec. Business Day, <http://www.nytimes.com/2014/02/27/business/target-reports-on-fourth-quarter-earnings.html>.
28. Osawa, Juro, "As Sony Counts Hacking Costs, Analysts See Billion-Dollar Repair Bill," Wall Street Journal, 9 May 2011, sec. Asia Technology, <http://online.wsj.com/news/articles/SB10001424052748703859304576307664174667924>.
29. Sherr, Ian and Nick Wingfield, "Play by Play: Sony's Struggles on Breach," Wall Street Journal, 7 May 2011, sec. Technology, <http://online.wsj.com/news/articles/SB10001424052748704810504576307322759299038>.
30. "2013 LexisNexis True Cost of Fraud Study: Merchants Struggle Against an Onslaught of High-Cost Identity Fraud and Online Fraud," LexisNexis, September 2013, <http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2013.pdf>.
31. Harrell, Erika, and Lynn Langton, "Victims of Identity Theft, 2012," U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, December 2013, <http://www.bjs.gov/content/pub/pdf/vit12.pdf>.
32. Ibid.
33. Munich RE, "Survey Shows Small Businesses Have Big Data Breach Exposure," Hartford Steam Boiler and Ponemon Institute, 6 March 2013, <http://www.hsb.com/HSBGroup/Subpage.aspx?id=579>.
34. New York State General Business § 899-aa. Available: <http://public.leginfo.state.ny.us/>
35. New York State Technology Law § 208. Available: <http://public.leginfo.state.ny.us/>
36. NYS Division of Homeland Security. "New York State Security Breach Reporting Form." 17 June 2013, <http://www.dhses.ny.gov/ocs/breach-notification/documents/State-Data-Breach-Form.pdf>.

Faculty Biography: Joe Ortego

Partner | Nixon Peabody | New York, NY

212.940.3045 | jortego@nixonpeabody.com
http://www.nixonpeabody.com/joseph_j_ortego

Joseph Ortego is the Practice Group Co-Leader of Nixon Peabody's Commercial Litigation Practice, as well as the chair of NP Trial®, an international team of the firm's most successful and experienced trial lawyers. He represents major private and publicly traded companies and their executives, having tried over 100 cases to verdict in both federal and state courts throughout the country and has successfully represented clients before arbitration tribunals around the world.

Joe is recognized by The Legal 500 as a leading attorney in the Litigation, Product Liability, and Mass Tort: Aerospace/Aviation categories, U.S. News & World Report as a Best Lawyer in Product Liability Litigation, Benchmark Litigation as a New York local litigation star, The Best Lawyers in America for his work in the practice area of Product Liability Litigation—Defendants, and Martindale-Hubbell Law Directory in its highest peer review ratings category, AV Preeminent. Additionally, Joe is included in New York Super Lawyers, based on peer review surveys, LGM Life Sciences as a "Life Sciences Star," and the Who's Who Legal Series for Life Sciences.

Services

- Automotive, Trucking & Fuel Systems
- Consumer Products
- Pharmaceutical & Medical Device Litigation
- Health Effects - Toxic & Complex Torts
- Environmental Litigation
- Aviation Product Liability
- Securities & Corporate Governance Litigation
- Insurance Litigation
- NP Trial®
- NP Second Opinion®
- Corporate & Finance
- Food, Beverage & Agriculture
- Food Safety Litigation
- Arbitration
- Class Actions & Aggregate Litigation
- Products: Class Action, Trade & Industry Representation
- Global Disputes
- Complex Commercial Litigation
- Financial Services Litigation
- Labor & Employment
- Litigation
- Insurance
- Labor & Employment Litigation
- Electronic Discovery & Digital Evidence
- Life Sciences

Education

- Boston University School of Law, J.D.
- Syracuse University, B.A., with honors