



TRENDS IN ELECTRONIC FINANCIAL CRIMES

Fraud Investigations Division:
Global Security & Investigations



Melissa Smart

Mid-West Manager,
Electronic Crimes
Investigations

JPMORGAN CHASE & CO.



Objectives:

- Provide a high level view of emerging fraud trends impacting the financial services industry and their customers
- Show how “old” fraud schemes have been updated to take full advantage of advances in and limitations of technology
- Demonstrate how the confluence of security, convenience, and strong customer service can expose vulnerabilities that are constantly shifting between channels





Fraud in 2013

- Fraud losses suffered by banks, businesses, and consumers continues to grow at an alarming pace
- As fraud prevention tools improve in one channel, fraudsters shift to other channels in an unending game of cat and mouse
- Personal and account information is the prize for criminals
- The source of the compromise is often outside of our direct control
- The criminals are motivated, well organized and adaptable



From this in 1980...

[illegible]

...to this today

JPMORGAN CHASE & CO.



2012 eFraud Global Forum: Industry Perspective

The majority of survey participants in the 2012 eFraud Global Forum indicated that the global economic situation resulted in an increase of online fraud, and listed the following as some of the reasons for the increased complexity of keeping up with fraud:

- vulnerabilities in the myriad of system components
- increased sophistication and unpredictability of cyber criminals and their willingness to collaborate with each other
- users are the weakest link – they are not motivated to protect their systems due to reimbursement policies
- overwhelming amount of “noise” that makes it difficult to drill down to the actual threat
- dynamic nature of the environment – always something new to learn and tackle

Source: eFraud Global Forum 2012 Fourth Annual Online Fraud Benchmark Report



2012 Internet Crime Complaint Center (IC3): Consumer Perspective

In 2012, the IC3 received 289,874 consumer complaints with an adjusted dollar loss of \$525,441,110¹, which is an 8.3-percent increase in reported losses since 2011.

Top 10 States by Count:
Victim Complainants (Numbered by Rank)



Age Range	Male		Female		Total Complaints	Total Loss
	Complaints	Loss	Complaints	Loss		
Under 20	107	\$41,700.10	138	\$61,780.58	245	\$103,480.68
20 - 29	550	\$303,823.15	684	\$328,612.34	1,234	\$632,435.49
30 - 39	654	\$988,770.08	802	\$553,109.25	1,456	\$1,541,879.33
40 - 49	695	\$798,809.47	872	\$953,741.15	1,567	\$1,752,550.62
50 - 59	727	\$1,862,651.23	802	\$1,766,926.91	1,529	\$3,629,578.14
60 & Over	781	\$923,423.49	422	\$1,293,565.28	1,203	\$2,216,988.77
Total	3,514	\$4,919,177.52	3,720	\$4,957,735.51	7,234	\$9,876,913.03
National Rank					9	13



Why are fraud losses on the rise?

- Organized and professional fraud rings are becoming more prevalent and sophisticated – global enterprises with key organizers in uncooperative countries
- Cyber-crime advances make it possible to quickly compromise large quantities of data
- The potential victims of fraud include millions of consumers
- Availability of customized malware has made this attack vector accessible to what had been lower level criminal enterprises
- Desktop publishing keeps counterfeiting relatively cheap and easy
- Risk Management is still too silo driven and does not adequately address cross channel threats
- Bad Economy



HARVESTING AND AGGREGATING INFORMATION

Where is our Information?

Wallets

Credit Bureaus

Medical Professionals

Loan Brokers & Closers

Government Agencies

Cell Phones

Public Records Databases

Payment Processors

Personal Computers

Social Media



NOVEMBER 2013 LUNCHEON



Global Payment Breach

WSJ MARKETWATCH BARRON'S SMARTMONEY ALLTHINGSD FIN FACTIVE MORE

Friday, March 30, 2012 As of 5:16 PM New York 70° | 58°

THE WALL STREET JOURNAL. BUSINESS

U.S. Edition Home Today's Paper People In The News Video Blogs Journal Community

World U.S. New York Business Markets Tech Personal Finance Life & Culture

Asia Europe Earnings Economy Health Law Autos Management Media & Marketing Enr

TOP STORIES IN Business

1 of 12 When Facebook Met Wall Street

2 of 12 The Many Hats of Aubrey McClendon

BUSINESS | Updated March 30, 2012, 5:16 p.m. ET

Data Breach Sparks Worry

Hack Attack at Card Processor Compromises Potentially Thousands of Accounts

Article

Video

Stock Quotes

Comments (82)



By ROBIN SIDEL and ANDREW R. JOHNSON

Concerns about credit-card security heightened Friday after a little-known Atlanta company disclosed it had been hit by hackers, potentially exposing hundreds of thousands of account holders to fraud.



Credit and debit card processor Global Payments has been hit by a security breach that has put some 50,000 cardholders at risk, Andrew Johnson reports on Lunch Break. Photo: Bloomberg News.

The breach at [Global Payments Inc.](#) [GPN -1.26%](#) is the latest in a wave of data attacks that have heightened consumer concerns about identity theft. The card industry has been particularly vulnerable to those concerns amid a slew of big breaches in recent years as more Americans choose to pay with plastic rather than cash.

The extent of the breach couldn't be determined and it wasn't immediately

clear if cardholders have seen fraudulent transactions. Consumers typically aren't liable

Twitter Hack

CNNMoney
A Service of CNN, Fortune & Money

FORTUNE Money

Home Video Business News Markets Term Sheet Economy Tech Personal Finance

Apple 2.0 Big Tech Tech Tumblr Innovation Nation Startups Brainstorm Tech Video

INVEST MORE OF YOUR MONEY IN YOU:

- ✓ No account service fees
- ✓ Low account minimums
- ✓ \$8.95 online equity trades¹

Other fees may apply

Twitter hack breaches thousands of accounts

CNNMoney

30 comments

By Laurie Segal @CNNMoneyTech May 8, 2012: 9:44 PM ET

NEW YORK (CNNMoney) -- A Twitter hacker on Monday revealed thousands of user names and passwords for the microblogging site, but here's the good news: Most of the compromised accounts appear to be spam.

Word of the breach began spreading Tuesday after hacking news and activist hub [Airdemon](#) posted a dispatch saying 55,000 accounts had been compromised. It linked to Pastebin pages containing the allegedly compromised user names and passwords.

Sponsored Links

LifeLock® Official Site
Identity Theft Protection Service.
Proactive Identity Theft Protection.

Google Apps for Business
Join more than 4MM businesses.
Mobile Email, Calendar, Docs

[Buy a link here](#)

A Twitter representative said the company is investigating. He also downplayed the extent of the potential breach, which hit a small sliver of Twitter's 140 million active users.

"It's worth noting that, so far, we've discovered that the list of alleged accounts and passwords found on Pastebin consists of more than 20,000 duplicates, many spam

accounts that have already been suspended and many login credentials that do not appear to be linked (that is, the password and username are not actually associated with each other)," Twitter spokesman Robert Weeks said.

Still, Twitter is taking precautions

Most Popular

Occupy Bank of Am

Fannie Mae doesi

Apple's stock is g

Ax won't fall on rur

10 housing marke

Tech Blog

APPLE 2.0

How Apple g

TECH TUMBLR

Confessions



2011 Data Breach Investigations Report

- Virtually all of the attacks were exclusively from external sources (95%)
- Only 2% involved exclusively internal sources
- The breaches involved various tactics: 1) Hacking 81%; 2) Malware 69%; 3) Physical Attacks 10%; 4) Social Tactics 7% ; 5) Privilege Misuse 5%
- The breaches were generally not sophisticated - 97% were avoidable through simple or intermediate controls.
- 85% of breaches took weeks or months to discover
- Use of stolen, default or easily guessable login credentials involved in 82% of compromised records
- Exploitation of backdoor or command and control channel involved in 49% of compromised records)

Source: 2011 Data Breach Investigations Report , Conducted by Verizon RISK, U.S. Secret Service, Dutch High Tech Crime Unit

Phishing Emails Still Work



NOVEMBER 2013 LUNCHEON

From: Chase Bank
Subject: Possible Account Problems
Priority: URGENT

An Important Notice Concerning Your Personal Information

Dear Chase Bank Customer:

We have recently noticed several attempts to log into your Chase Bank account from a foreign IP address. We have reasons to believe that your account may be compromised by a third party.

However if you are the rightful Account holder, click on the link below and login as we try to verify your identity:

<https://chaseonline.chase.com/>

We ask that you allow at least 48-72 hrs for the case to be investigated and we strongly recommend not making any changes to your account in that time.

The information contained in this notice contains some terms we are required to disclose to ensure that we comply with privacy laws. If you have any questions about the information contained in this notice, please call us at (212) 334-0555 or write to: Chase Bank, 231 Grand St, New York, NY 10013.

Other Phishing themes:

- Job Opportunity
- Romance
- Inheritance
- Unclaimed Property
- Guaranteed Loans

Additional Enticements:

- Offer a \$25 account credit for the inconvenience
- Offer a free “Fraud Busters” enrollment

Dear Name of Recipient

A complaint has been filled against you and the company you are affiliated to by Mr. George Hanson and sent to Federal Trade Commission by fax in witch he's claiming that he has been cheated by you and your company in paying a greater amount of money than the one appearing on the invoice you gave him for using your services.

The complaint states he contacted your company on MON,22 OCT 2007, trying to solve this situation without interference from any Governmental Institution , but your company refused to take action.

On WED,24 OCT 2007, the complaint was sent by fax to Federal Trade Commission and we forwarded it to Internal Revenue and Better Business Bureau.

Complaint was filled against :

Name : Name of recipient

Company : - Company Name

If you feel that this message has been sent to you in error or if you have any questions regarding the next steps of this process, please download the original complaint by clicking the link below :

http://ftc.gov/fraud/complaints/24_oct_2007_george_hanson.doc

Please take knowledge of the complaint's content and complete the form at the bottom of forward it to fraudcomplaint@ftc.gov.

Bruce Jameson

Complaint Officer

Phishing with new bait



NOVEMBER 2013 LUNCHEON



New Group in Chicago: Crackin' Cards

- Recruit willing participants
- Purchase debit cards/PINs
- Counterfeit check deposits
- Cash Out at Wal Mart, Currency Exchange

Recent Development:

- Chase employee card involved





Malware 101

MALWARE (Malicious Software)- software designed to harm or secretly access a computer without the knowledge of the owner.

Distribution

- Hacked websites distribute malicious code
- Email attachments
- Peer-to-Peer file sharing networks
- Person-to-Person: (CDs, Flash Drives, etc.)



*“Since 2005, there have been significant changes in the threat landscape... malware can compromise some of the most robust online authentication techniques, including .. **multi-factor authentication** “*

FFIEC Supplement to Authentication in an Internet Banking Environment - June 28th, 2011



Device Spoofing

- Device ID (DID)- Unique cookie downloaded on a device as one form of authentication
- Some malware copies, or “spoofs”, the DID from an infected computer
- When placed on a different device, that now appears to be an authorized DID for that banking customer
- Malware also harvests user IDs and passwords for any accounts that are accessed from that computer though key logging (email, bill websites, etc.)
- Provides all the pieces that a fraudster needs to steal your money





Malware/Spoofing Defeats Dual Token Authentication

- Corporate CFO/Treasurer targeted through email address on business website
- Email phishing results in malware downloaded on a computer
- Keylogger component of malware transmits initial banking login credentials back to the criminal
- Monitoring of email identifies the secondary security administrator
- Coordinated phishing email delivery prompts users to attempt login using secure tokens
- Fraudster executes a man-in-the-browser attack taking over online both sessions
- Fraudster creates wire from 1 user account, approves and releases from the 2nd account
- Users unable to terminate sessions



Business Threat: ACH Transfer Fraud

With access to just a businesses account and routing number, a criminal can electronically steal their money without having to directly access the account

- Two accounts at different financial institutions (one belonging to a suspect and the other to a victim) can be linked through the confirmation of trial credits
- Trial credit amounts for business accounts can be easily verified through a VRU or telephone banking
- Once verified, an ACH “pull” is requested from the business account
- Risk tools are not focused on pull activity due to NACHA return rights



Simple Identity Theft: Felony Lane Gang

Identity Theft:

- Victim's wallet is stolen- debit card identifies bank of choice
- Criminal makes an ID with the victim's information but the photo of their chosen "casher"
- Criminal uses telephone banking to verify account balances and obtain the last 4 digits of the victim's account number(s), check for account alerts, etc.
- Cashier visits multiple branches in quick succession cashing checks of other victims or completing cash withdrawals
- No cash in the account? No problem! Cashier will deposit checks stolen from other victims to inflate the balance first





Check Images Available Online

The convenience of online check images has made it easier for criminals:

- In late April 2012, Trusteer uncovered an elaborate - but relatively easy to pull off - check-hijacking scheme where hackers relied on phishing attacks and malware to access online accounts to retrieve check details.
- A similar scheme involving check images cropped up in August 2010, when federal investigators discovered hackers in Russia had breached an online check-image database managed by a third-party.



Ref: Infosecurity.com "Check Fraud: The Next Generation" by Tracy Kitten

BRAVE NEW WORLD

THE RACE TO EVOLVE: MOBILE FRAUD



Mobile Threats

“Fraud over the mobile channel is a new entrant to the Top Attacks category”

-eFraud Forum 2012 Fourth Annual Online Fraud Benchmark Report

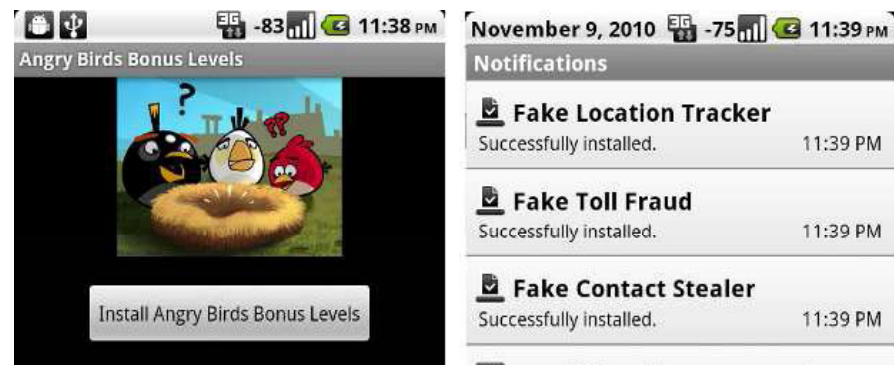
Androids are the most targeted OS

Android Threat Growth



The increase in the number of detections in the latter part of 2012 was due to the rise of high-risk apps.

Source: TrendLabs 2012 Mobile Threat and Security Roundup

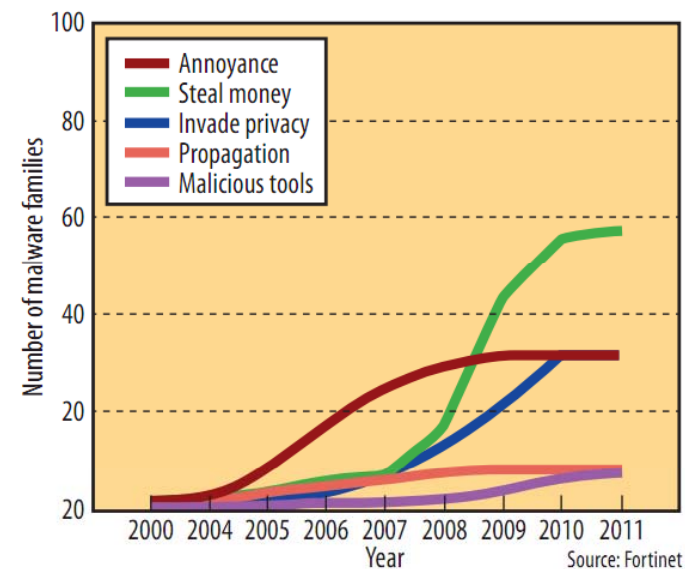
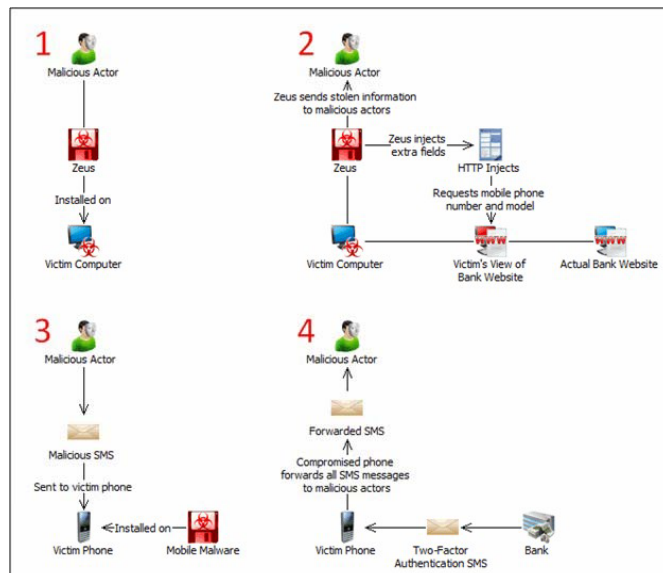




Mobile Threats

- Although all smartphones can be infected, if you use an Android smartphone you are now 2.5 times more likely to encounter malware (malicious software) than you were six months ago
- This year, 30% of Android users are likely to encounter a web-based threat such as phishing scams, "drive by downloads" and browser exploits

<http://www.cnn.com/2011/TECH/mobile/08/04/lookout.threat.report.gahran/>





Mobile Technology

Break-neck speed of business and product innovation is matched, and often out paced, by evolution of fraud tools

New Chase products: Popular with customers... and criminals!

- Quick Pay

Use an email address to send payment to another party



- Quick Deposit

Deposit checks into your account using your phone's camera






Mobile Technology

Square

- Created in 2009 by the founder of Twitter
- Card reader plugs into headset jack of a smartphone and creates a mobile credit card reader
- Prospective vendors register online to request approval to use and establish end-point banking information
- Designed to allow small businesses the ability to accept card payments without contracts, expense, and hardware required with traditional card processing
- Square swipe terminals available at many retailers

Now everyone can accept credit cards.

Accept credit card payments on your Android, iPhone or iPad with the free Square Card Reader. You'll never miss a sale again.



Fast Setup
Just sign up and install the app to begin accepting payments. Within minutes.

Free Card Reader
We'll mail you a free Square Card Reader to plug into your mobile device. [Learn more](#)

One Simple Rate
Only 2.75% per swipe for Visa, MasterCard, Discover and American Express. [Learn more](#)

Next-Day Deposits
Take payments during business hours and we'll deposit your funds the next business day. [Learn more](#)

iPhone Android

MANAGING THREATS FROM MULTIPLE CHANNELS

Factors for Protecting Customers



NOVEMBER 2013 LUNCHEON



The Authentication Challenge

- Customers enter the Bank through multiple product and service channels, historically with a silo view of the risks in their application
- As customers use more products and their products are linked more conveniently, the risk across product and service channels is shared
- Remote channels, such as online, mobile, and telephone banking all require various levels of identity authentication
 - Social engineering/availability of personal information
 - Out of wallet questions are beatable
 - Innovations such as voice or keystroke biometrics are evolving
 - Even the token-based challenge authentication systems can be defeated by sophisticated malware and determined fraudsters
- Setting appropriate enterprise-wide authentication standards uniquely challenging
 - Must be strong but not too cumbersome for the customer
 - May be cost prohibitive



Intelligence Gathering

- Detect existing and emerging threats to the payment system
- Monitor and track the underground cyber fraud markets
- Identify and analyze exploitation techniques
- Engage criminals and recover stolen data
- Feed information back into risk models to learn the origin of stolen data
- Proactively protect customer accounts from future fraud incidents



Investigation Techniques

- Focus investigation priorities on grouping common fraud incidents
- Analyze fraud incidents for common points of compromise:
 - Same phone numbers and device IDs making inquiries
 - Employees accessing customer profiles
 - Common external purchase points
 - Common credit acquisition or other touchpoints
- Aggressively pursue protection for customers with common indicators prior to a fraud incident
- Partner with law enforcement and other impacted financial institutions
- Critically analyze internal controls and processes and recommend risk management solutions



Customer Education

- Create awareness in commonly visited spots
 - Prominent on websites
 - Statements and other periodic mailings
- Provide alert tools for customers to identify unusual activity
- Encourage reporting of suspicious activity with easy methods
- Follow-up when significant incidents occur and help customers diagnose their issues and remediate the source of the problem
 - Use fraud professionals for a deeper assessment



Contact information:

Melissa Smart

614-248-3057

Melissa.b.smart@jpmchase.com

THANK YOU!