

The Faces of Fraud: An Inside Look at the Fraudsters and Their Schemes

Tom Field & Erik Rasmussen

BankInfoSecurity, US Secret Service

Session ID: HT1-401

Session Classification: Intermediate

RSACONFERENCE 2012

Faces of Fraud

What Are Today's Top Schemes?

- ACH/wire (account takeover)
- Check
- Credit/debit card
- Insider
- Phishing/vishing
- Third-party POS skimming

(answers later in presentation)





Agenda

- 2012 Fraud Trends
- From the Trenches: US Secret Service on the crimes, criminals and investigations.
- Latest Research: Sneak peek at 'Faces of Fraud' survey results.
- Summary: What you can do.



2012 Fraud Trends

- ATM Crimes skimming of machines, as well as vestibules;
- POS Skimming Michaels, Save Mart, pay-atthe-pump;
- Insider Threat CitiGroup = \$22 million; UBS = \$2 billion;
- Organized Crime NYC indicts 111 'Biggest ID Theft Bust in History.'





2012 Fraud Trends (cont.)

- Dueling Lawsuits Re: corporate account takeover, one court rules in favor of bank; another rules for customer.
- Regulatory Guidance FFIEC tells banking institutions to crackdown on online fraud.





2012 Fraud Trends (cont.)

FFIEC Authentication Guidance:

- Assess Risks;
- Deploy Layered Security;
- Improve Authentication;
- Educate Customers.
- Examinations begin now.



From the Trenches

US Secret Service on the crimes, criminals and investigations.





About Erik Rasmussen

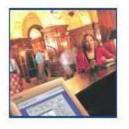
Erik Rasmussen has been a Special Agent with the United States Secret Service ("USSS") since August 2004. He is currently assigned to the Criminal Investigative Division, Cyber Intelligence Section. Prior to this assignment, he worked on the Electronic Crimes Task Forces for the Los Angeles and Seattle Field Offices.





Payment System Attacks













Primer

- Also known as "point of sale hacks" or "point of sale attacks", these intrusion incidents are becoming an all too frequent occurrence
- Common in retail, food and beverage, and hospitality industries
- Most common operating system (OS): Windows!
- Most common password: "Password1"
- Parties involved
 - Card brands
 - Issuer
 - Acquirer
 - Merchant
 - Cardholder



Credit Card Authorization Cycle

card swiped at terminal \rightarrow merchant accepts data, sends to acquirer \rightarrow acquirer checks in with issuing bank to verify card \rightarrow card network verifies data with issuing bank > issuing bank approves or denies card \rightarrow card network notifies acquirer of response → acquirer notifies merchant of response \rightarrow merchant completes transaction





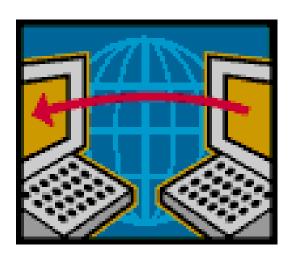
Cardholder Data: What is Exposed?

Card Present

- -face to face
- -mag stripe swiped
- -PIN on debit transactions

Card Not Present

- -internet
- -phone/mail
- -Primary Account Number, expiration, CVV, contact info

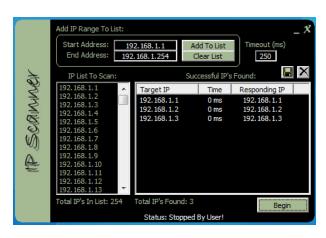




Numbers Don't Lie!

- Food and beverage accounted for most of the breaches in 2011
- Hospitality breaches are on the rise
- At the bottom? Construction, Entertainment, Education industries
- Software-based POS systems are 75% of the breaches
- Targets of opportunity
 - Attackers scan IP ranges
 - Open source internet searches for commonly used usernames and passwords
 - Target rich environment (terminals are everywhere)
 - USB enabled (walk right up and hack away!)









Anatomy of a Breach

- Ingress
 - How did they get in?
- Collection
 - How/where is the data stored and/or compromised?
- Egress
 - How/where is the data sent?





Ingress

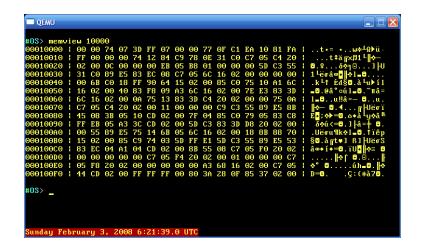
- Remote access is the most common method (back of house server or at the terminal itself)
- Default credentials often not altered after installation
- Firewall rules relaxed
- Firewall rules absent

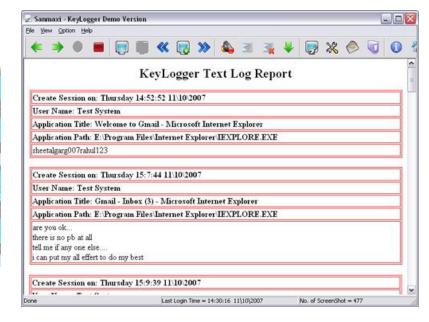


Collection

- Malware
 - Memory dumper
 - Keylogger
 - Network sniffer
 - Anti-hacker hacking tools

205	SMIN CO.	bookson.	- Street,	*PD-11/2 077/2 0/07/06/07/2 04/
1 T 6 000000	18 10 29 7	120100-0-25	265	Timbrid yang AM sixtyprioritie (Lastinum Lie
C2 6,000HK	979,76,8,00	- GR. 111.09.79	- DKE 111	Combind spery requires DOM all directional in mechanism and DAM all Circ. excessor and
3.0.16203	GR. 1117.70.70:	1117-10-16-20	. 665	Conduct party A bibliography and Cl. attentions con
- F. H. 1889	SP2, 94, 4-20.	10.10.76.76	- 886	resource garry response DAME as directional or automate and DAME at the automate rim a 21 Jil Tile III.
3.5.1059	38.107.75.77	77-TI (55-75	or Marine	-BACK V DYTAL TOTAL SADAR MANDRES SAME MENTAGE TYPINGTHESIS TOTAL WINE.
3.2.1800	TR.10179/76	TO-D 408-79	108	4945 × MILE DESCRIPTION DESCRIPTION DESCRIPTION PROPERTY FOR PARTY.
3.83800	100,000,000	75.75.756.79	O107130	SECT A STATE THAT AREA WANTED AND REPORT THAT PARTY THE WANTED
8.26.1£780	SEC. 111.79.79	100.06.0.20	366	Contact party Adm County-Service, cl. admires, and
9 10 12000	579.36.4.26	18.10.29.29	MI	Visited party require 0000 at investment of excession on the at the excession on
10 14 110005	38.107.09.00	122 (0.0.16	-	State of the Control
111.79, 129400	577.36.A.29	200,000,000,000	960	Standard query response CAME and directioned in ampointed, spin CAME and the executation call A 13, 131, 134, 40
11 29,12090	38 GU-9CH	76.01.006.00	IN SECURIO	Title y folgs: John have starting laser Mindell Traveled CO Travel Size.
- 12-20-1100Au	34:00:30:70	TOTAL SHEET	ICENTON.	Title o being field from storage committees the constant of the storage
14 2th 980000	10111-04-01-08-01	PO. 11 (00) 11 (11 (11 (11)	1886	We had at 10 10 10 10 10 10 10 10 10 10 10 10 10
11 (9.3400)	70.11.05.17.11.00	10135 (0036) 40.40	LARRY LA	WHIT IN A LEAST ROTH ON THE STATE
. 16 3D, 13006	26 (11.29, 20.00)	STRUCTURE STRUCTURE	COMPANY	THE A ROLL LINE SOLD SOLD WATER LINE WATER THAT THE PROPERTY THE ROLL AND
11 10,14060	18,111,03,19	B-100.56.4	M25.	WP (Lief)
IR M. DOM:	DC1D-36-79	100 M. N. 29	1960	Wartlerf query date Explorerise Lie of Internate Lies
14 LC Livery	100 M A 10	16-117-29-79	-	Contact party respect DAM of distributed in document and DAM (1) is a manager and
28 St. 13890*	36.101.79.79	100,700,00,00	- March	STANDARD GRANT A MANAGEMENT OF AN ARREST AND ADDRESS OF THE ARREST ADDRESS OF THE ARREST AND ADDRESS OF THE ARREST ADDRESS OF THE ARRE
31 M. 10000	22.0.00	26.03.95.9	90	Street gary register OWE 43 directured is also then, be CMM 13 5 is excelled use 4 O. III. III. III.
21 10 UOGA	SR 1117-79-79	77-71-201-10A	1255	THE VALUE AND ADDRESS OF THE PARTY OF THE PA
TE by Diebs	90.111.70.76	770-71-201-1HE	0.000	DOSC - Major COST Series SCHIERE SAME MERCONS TRA-COMPANIES TERMS WINE .
14 to 1960p	10.141.75.75	77-71-00-111	O PERSON	NAME & STREET, TOTAL SOURCE MARKET SAME STREET, THE PROPERTY OF THE PARTY OF THE PA
25.80 (Chaoc)	100,117,175,770	CONTRACTOR STATE	100	COMMENT MATE AND PROPERTY OF A PROPERTY OF
35.61,12009	279, 18 A 19	100,000,000,00	98.	Water and control own in Control of Section 19 Control of Control
.IT MIPON	36.111.79.79	177,94 9, 23	MI.	Wanted garry 4 633 (printed time of property con
28 (0.10)(0.0)	579,79-8-20	14:111.79:79	1986	Hardest surry regions OWE of directional or assessment for OWE of the assessment one A.H. St. III. III.
H III LIPON	200000000	75-86-90-784	OF REPORT OF	SEAS of Arrigan (PM), happer belonging over the Contract Terrelationary Territorial attention
TR 16, 19550	200.000.29.29	Pr. H. (80-10)	100	Marc & Street (1990) Super Recomme cases retricing Transportation (1990) about
71 W. LEON	10171.04180.4050	CRUTH IN THE STATE OF	LAR	West Sea 198, 527 798 571 7655 144, 123, 786, 78
[11 Mt. 13000]	76-07/07/07/05	CHUMBING:	NAME .	TRACTOR A AS IN THE PARTY.





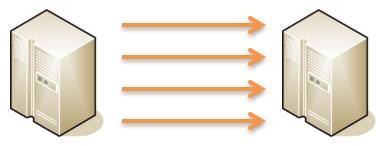






Egress

- Auto export functionality
- FTP servers (s) embedded in the malware
- Email account(s) embedded in the malware
- Transfer to a USB device if in person
- Numbers are evenly distributed
 - Nearly half of breaches involve malware egress methods





"SUBWAY" CASE







CEZAR BUTU



IULIAN DOLAN

- -Romanian citizens (2 arrested in the United States, 1 arrested in Romania)
- -Hundreds of Subway locations compromised
- -100,000 cardholders exposed
- -Actual fraud loss: approximately \$20 million
- -United States Secret Service, Manchester, New Hampshire office involved (1 agent)
- -Ingress method: RDP exploitation
- -Collection method: keystroke logger
- -Egress method: FTP server(s)



I'm Compromised...what's next?

- Is it an employee, social engineering, remote access?
- Law enforcement installs sniffer to monitor all incoming and outgoing traffic and images media to identify malware and stolen data destination.
- Merchant hires third party forensic firm and agrees to provide information to USSS.

What is critical to catch them?

- Prosecutorial involvement
 - Grand Jury Subpoenas
 - Court Orders
 - ECPA Search Warrants
- Obtain consent for full content monitoring
- Engage victim merchants early and keep them involved in case.
- IP address log analysis to identify important targets to monitor and confirm if the same hacker using multiple identities



What is critical to catch them?

- ECPA Search Warrants and PEN Registers
- Liaison with Law Enforcement in suspected countries
- Liaison with banking institutions

Latest Research

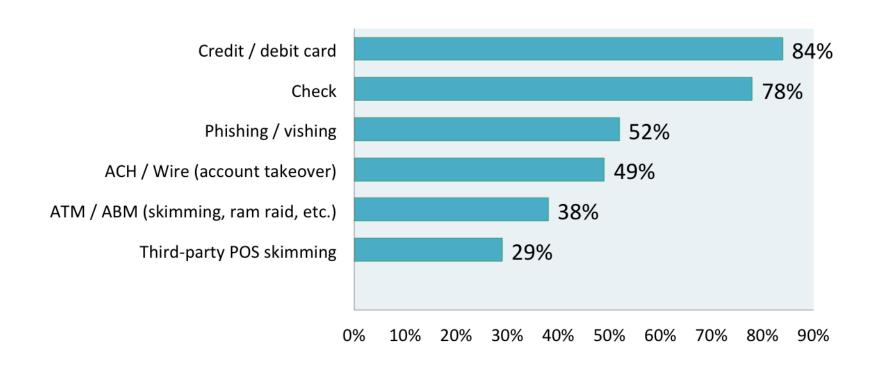
2012 Faces of Fraud Survey: Sneak Peek

Early look at preliminary results from our ongoing study

- Annual study
 - In the field
 - 89% US
 - 95% FI



What Are Today's Top Schemes?

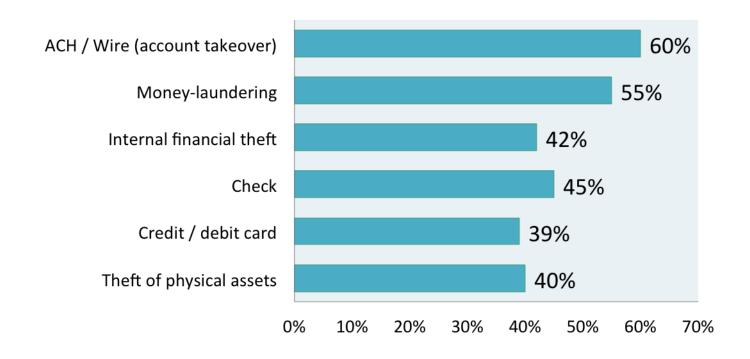


Check and payment card fraud remain top threats ...





Which types of fraud are you best prepared to prevent and detect?

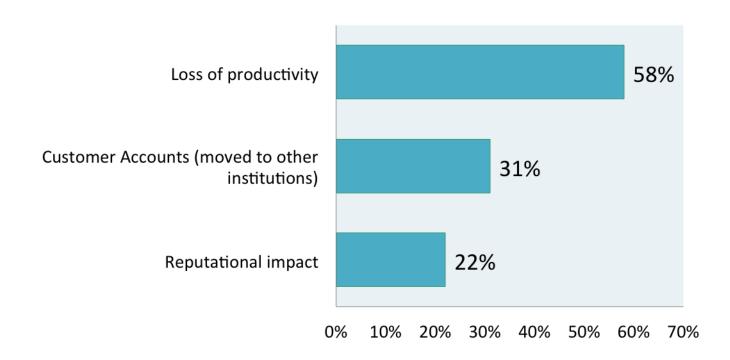


... but banks are best-prepared to defend against other risks.





Which non-financial losses did your organization suffer?

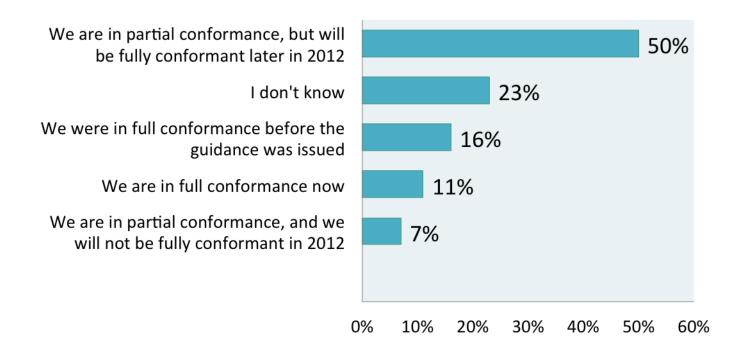


What price do you put on reputational loss?





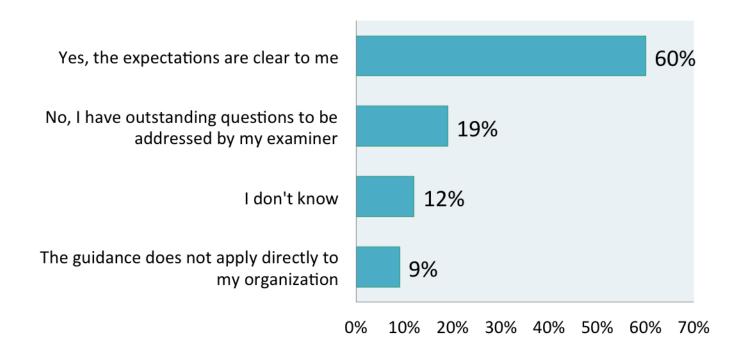
FFIEC Guidance: How do you assess your conformance?



Nearly ¼ don't know if they conform?



Do you fully understand the FFIEC's expectations?

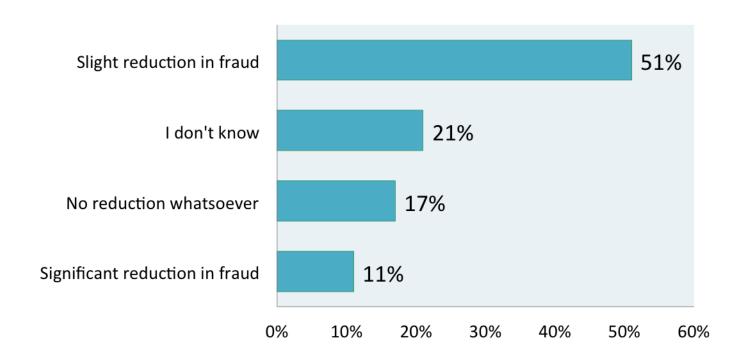


Nearly one-third do not understand expectations.





Will the FFIEC Guidance help reduce online fraud?

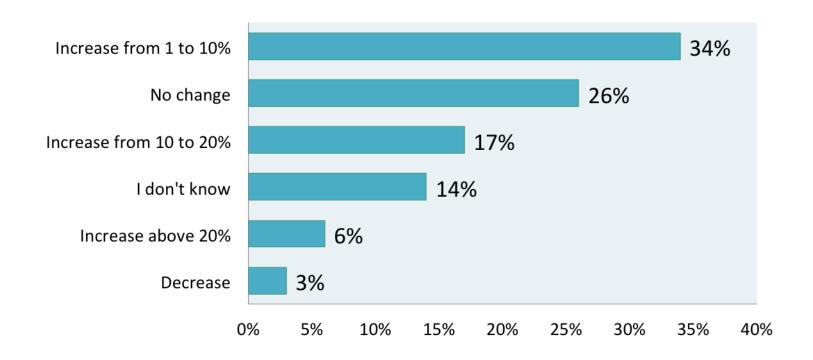


Barely 10% foresee a significant reduction in fraud.





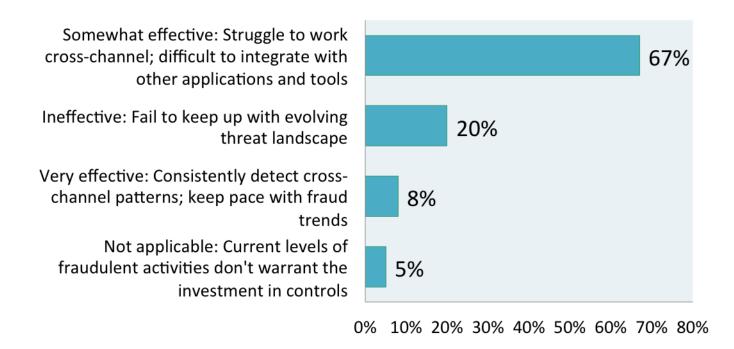
How will your anti-fraud resources change in coming year?



57% expect budget/staff increase.



How effective are current anti-fraud security controls?

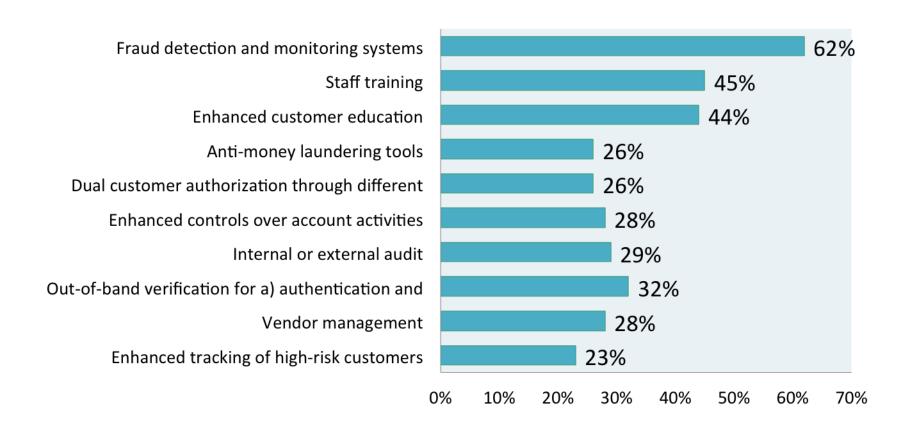


87% find controls somewhat effective or ineffective.





Investments over the next 12 months?



Fraud monitoring, staff training are top priorities.





Summary

- Top Fraud Schemes: It's all about vulnerabilities – threats are evolving;
- Law Enforcement: Work with agents at every level;
- Latest Research: FFIEC Guidance is a start, not a finish. Need to make smart investments.



What You Can Do

- Stay Current: Fraud schemes evolve daily.
- Raise Awareness: Employees, customers need to know the latest threats. Knowledge is security.
- Take Action: FFIEC Guidance is not for banks only – risk assessments, layered security and enhanced awareness are good for all entities.





Take the Faces of Fraud Survey:

2012 Faces of Fraud Survey: Complying with the FFIEC Guidance

Be a Part of New Study on Today's Top Threats







Take the Survey Now!

http://www.bankinfosecurity.com/surveys.php?surveyID=11

