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

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-at-the-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

micros®

Radiant® SYSTEMS

xpient SOLUTIONS

FireFly TECHNOLOGIES

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 →

merchant accepts data, sends to acquirer →

acquirer checks in with issuing bank to verify card →

card network verifies data with issuing bank →

issuing bank approves or denies card →

card network notifies acquirer of response →

acquirer notifies merchant of response →

merchant completes transaction

Cardholder Data: What is Exposed?

Card Present

-face to face

-mag stripe swiped

-PIN on debit transactions

Card Not Present

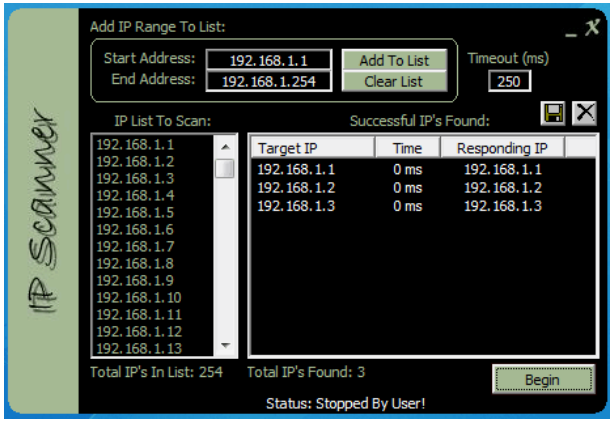
-internet

-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

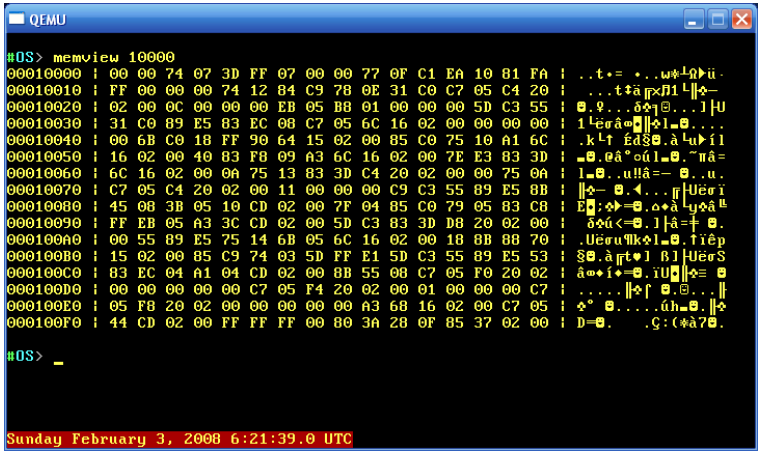
- Ingress
  - How did they get in?
- Collection
  - How/where is the data stored and/or compromised?
- Egress
  - How/where is the data sent?

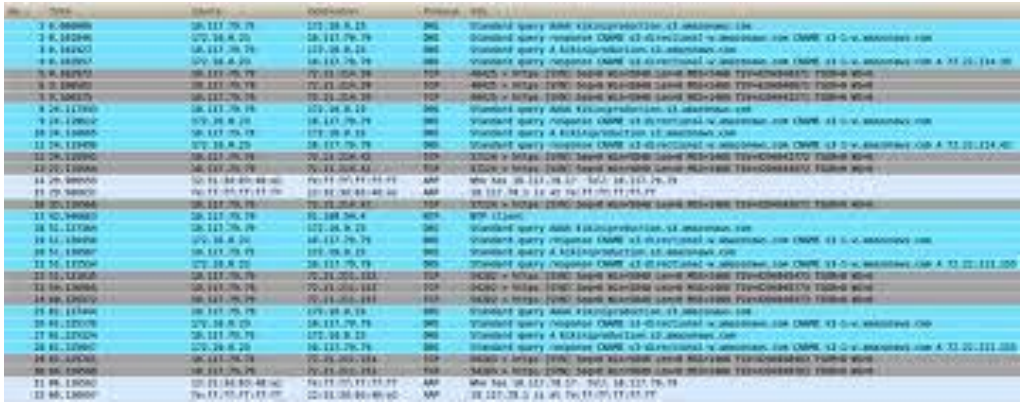
Ingress

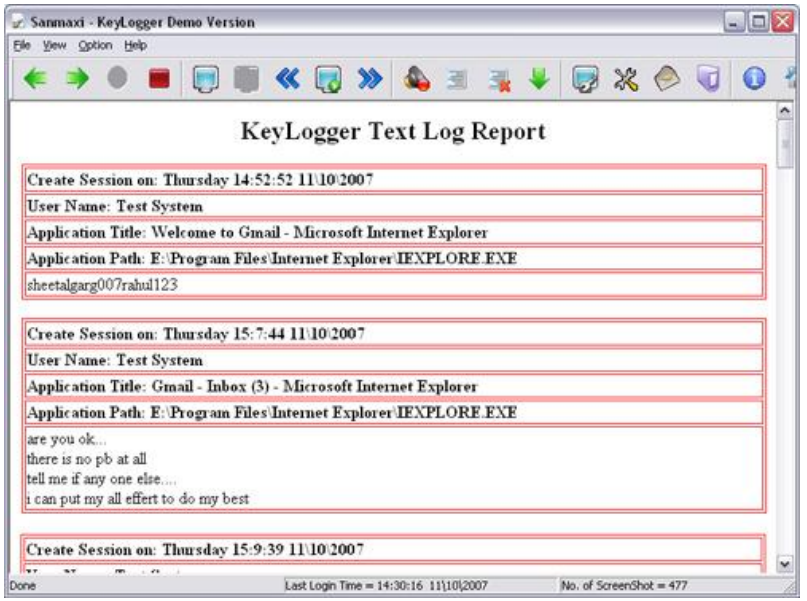
- Remote access is the most common method (back of house server or at the terminal itself)
- Default credentials often not altered after installation
- Firewall rules relaxed
- Firewall rules absent

Collection

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

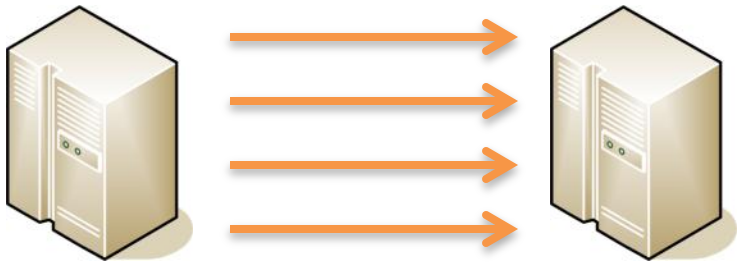




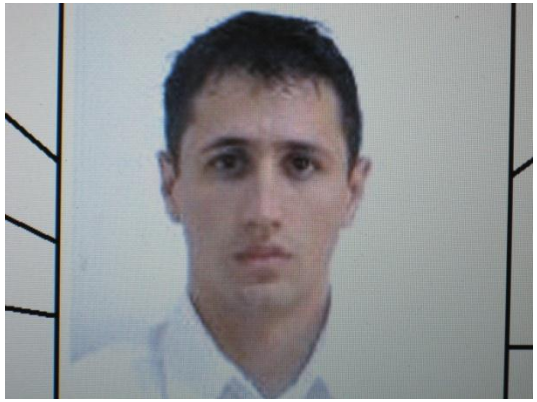


Egress

- 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



ADRIAN OPREA

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

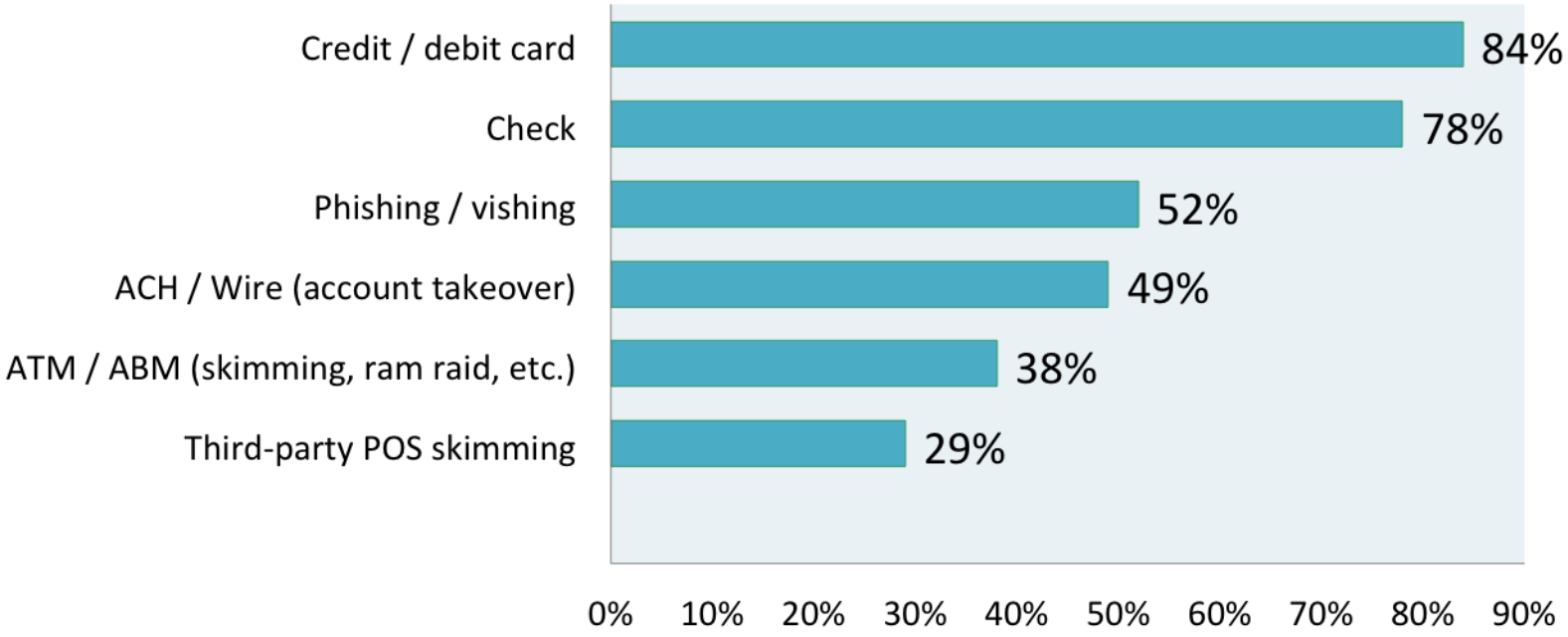
Latest Research

2012 Faces of Fraud Survey: Sneak Peek

Early look at preliminary results from our ongoing study

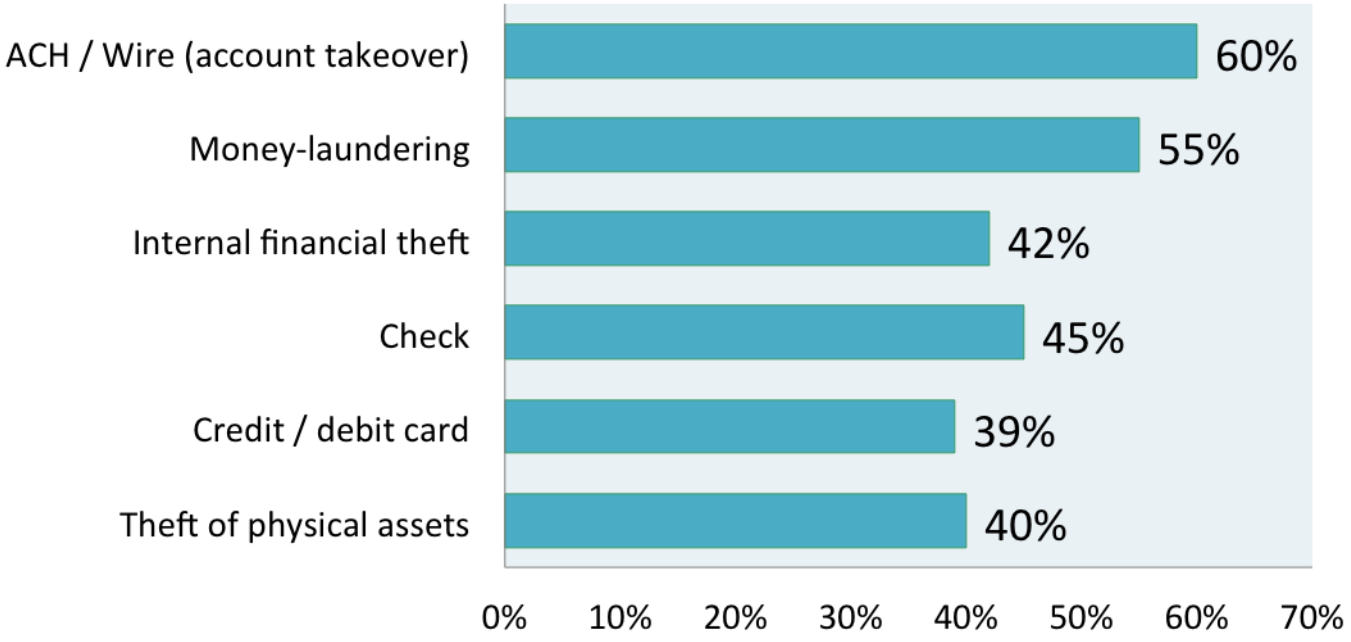
- **Annual study**
- **In the field**
- **89% US**
- **95% FI**

What Are Today's Top Schemes?



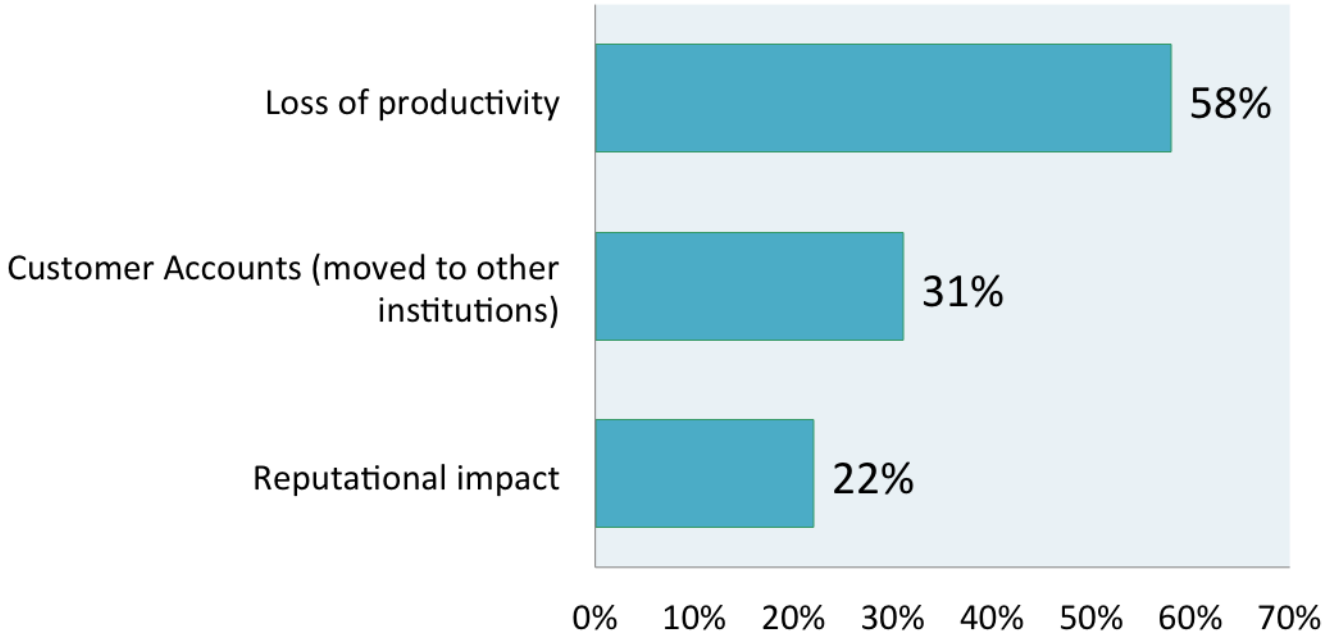
Check and payment card fraud remain top threats ...

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



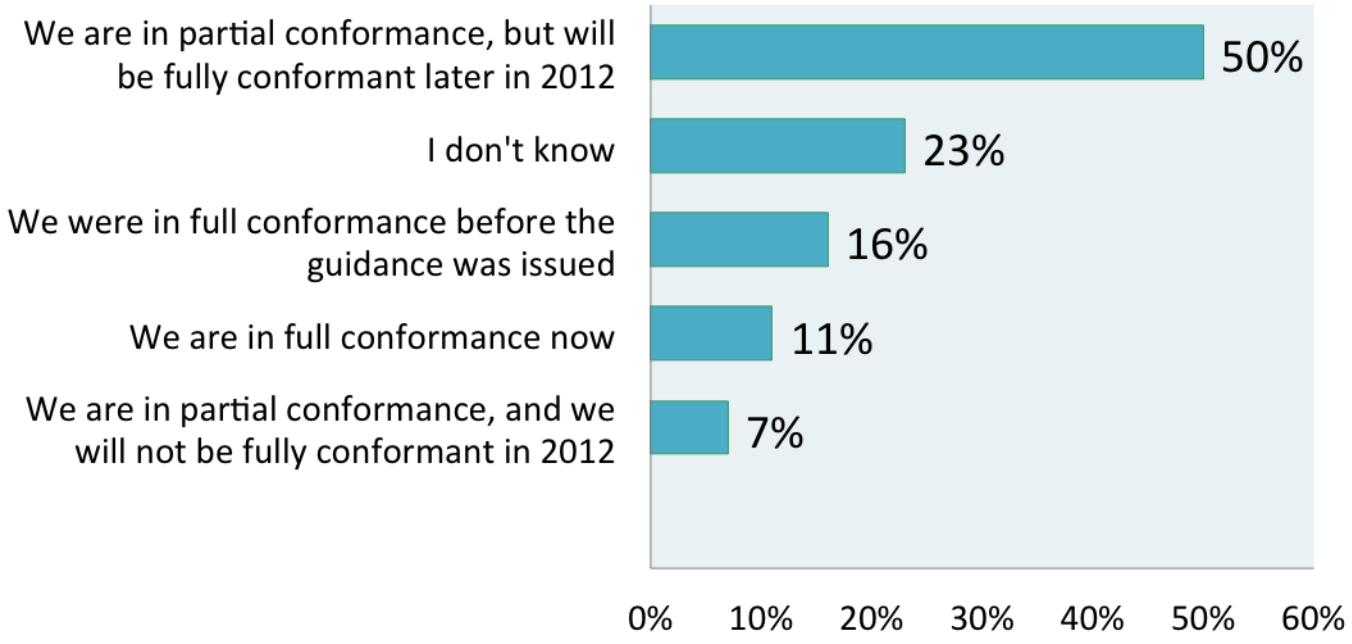
… but banks are best-prepared to defend against *other* risks.

Which non-financial losses did your organization suffer?



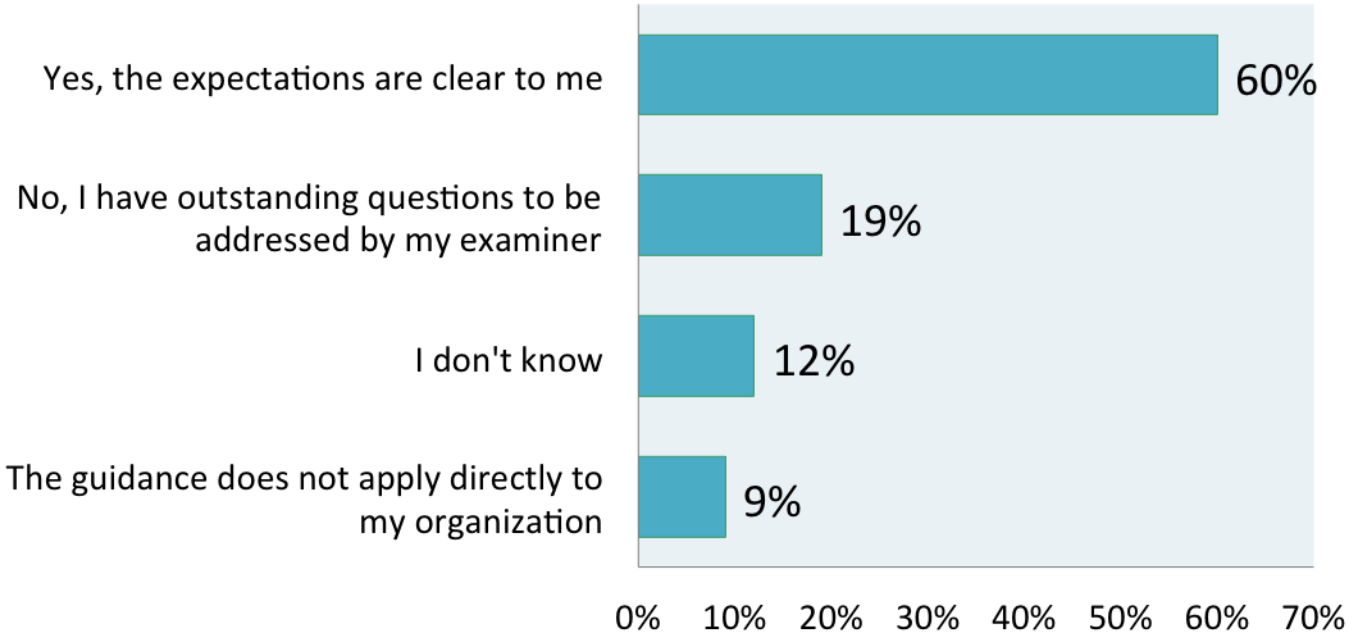
What price do you put on reputational loss?

FFIEC Guidance: How do you assess your conformance?



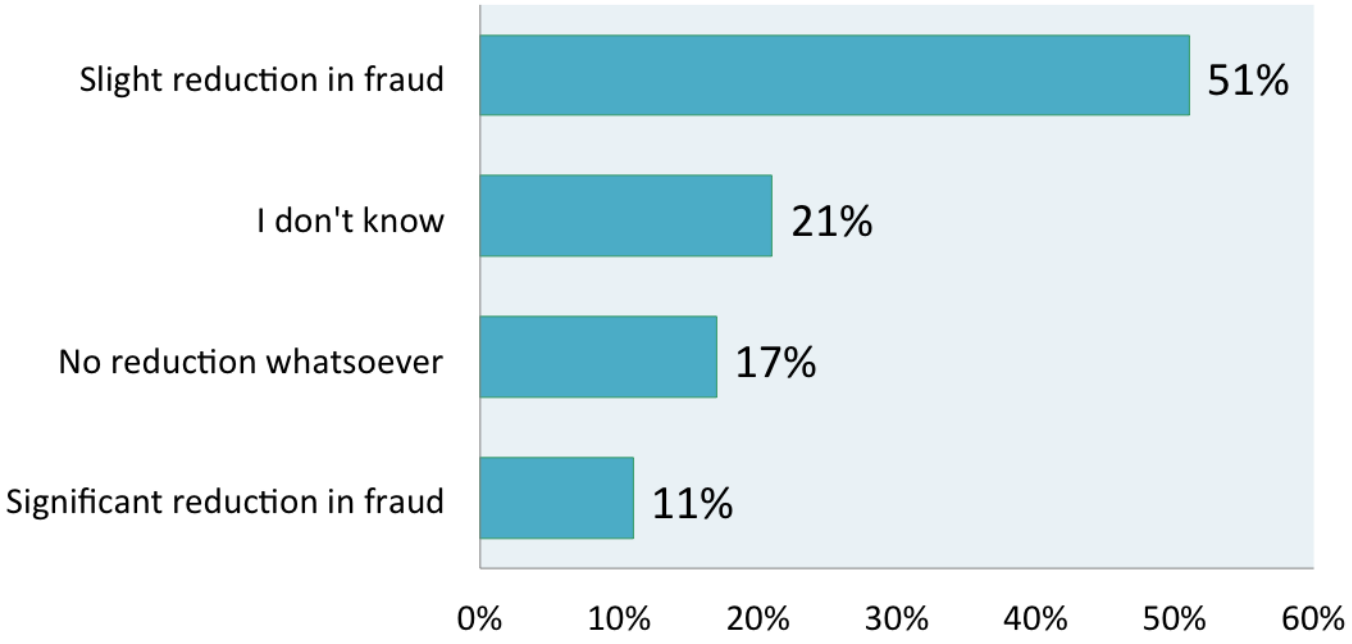
Nearly ¼ don't know if they conform?

Do you fully understand the FFIEC's expectations?



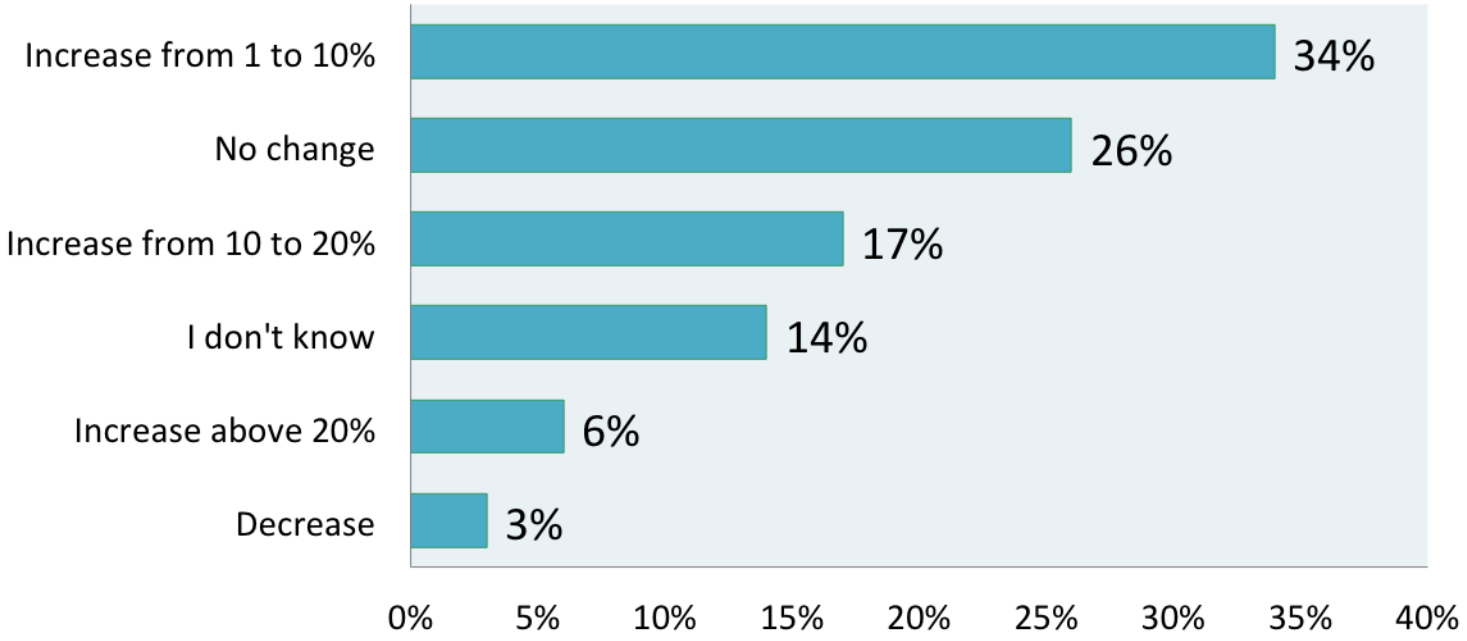
Nearly one-third do not understand expectations.

Will the FFIEC Guidance help reduce online fraud?



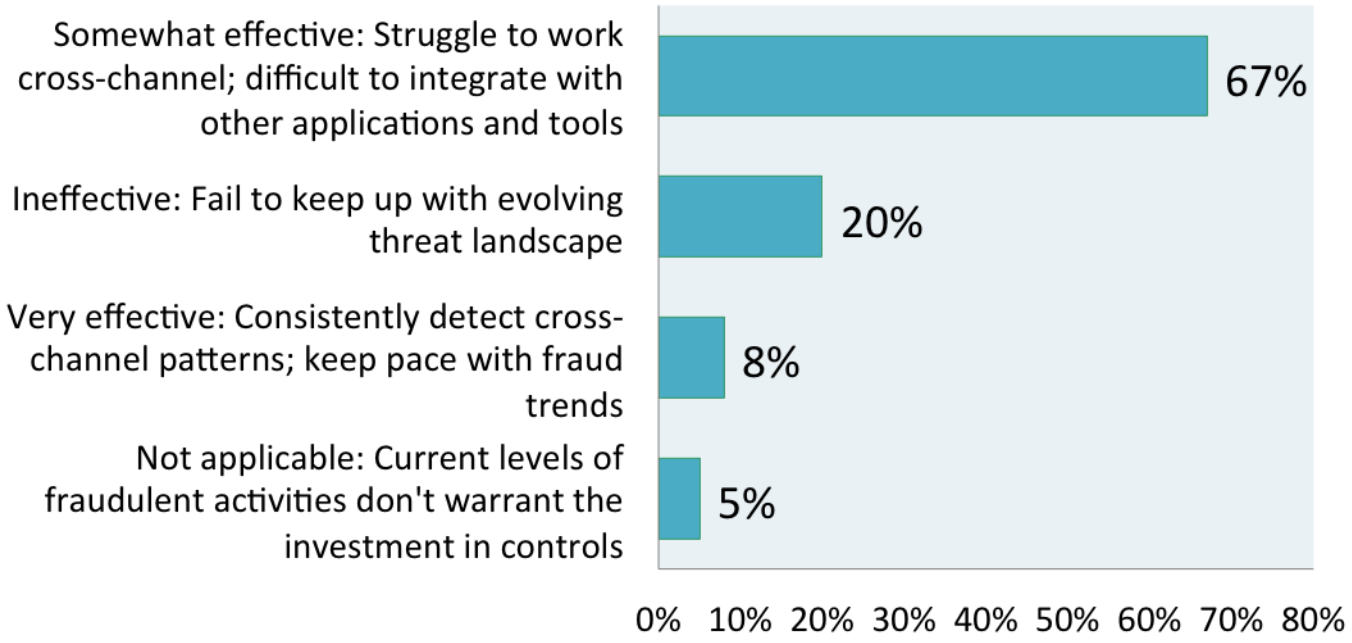
Barely 10% foresee a significant reduction in fraud.

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



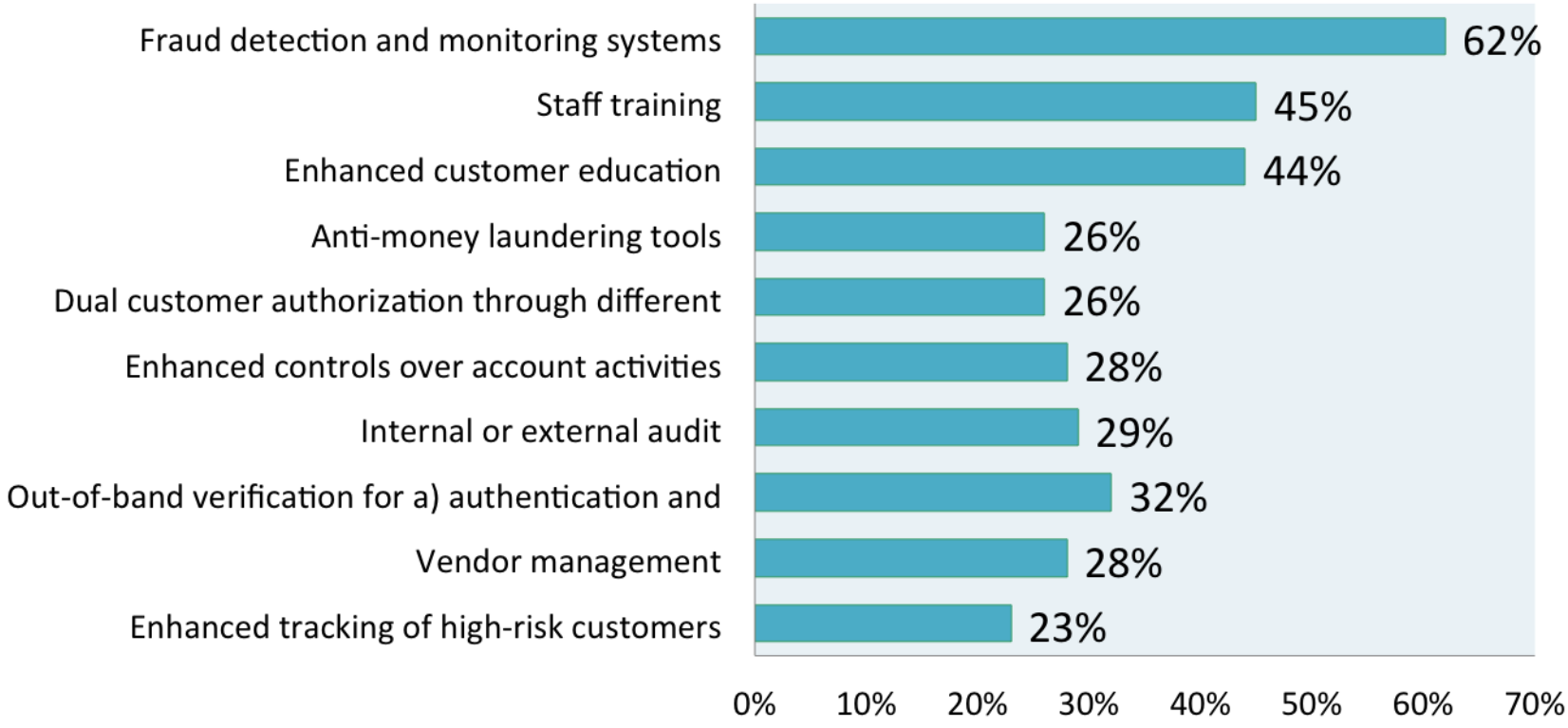
57% expect budget/staff increase.

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