Are you a Fraud Prevention Guru?

Do you know what it takes to protect your financial institution and your customers from ACH Fraud, Malware, and more? Take this short quiz to test your fraud knowledge, and learn tips to help prevent fraud before it happens or detect it quickly if it does.
1. What was the total amount of direct fraud losses incurred by US financial institutions in 2009?
   - $18 million
   - $180 million
   - $1.8 billion
   - $18 billion

2. How much has annual stolen card volume grown since 2005?
   - 50%
   - 113%
   - 221%
   - 1075%

3. What type of fraud causes the most severe losses, according to a poll of financial institutions?
   - Counterfeit credit/debit cards
   - Identity Theft
   - Malware
   - Skimming
4. While most types of new account fraud decreased in 2010, what type increased?

☐ Checking and savings accounts
☐ Credit Cards
☐ Internet Accounts (such as eBay and Amazon)
☐ Loans

5. ACH fraud does not contribute significantly to financial institutions’ fraud concerns—either through number of attacks or dollars lost.

☐ True
☐ False

6. In 2010, at least one bank account was compromised in how many households?

☐ 1.1 million
☐ 1.6 million
☐ 2.2 million
☐ 2.5 million
7. While ATMs aren’t exempt from fraud, they’ve been relatively fraud-free to date.

☐ True
☐ False

8. What percent of global consumers feel that mobile phone payments increase the risk of identity theft and fraud?

☐ 25%
☐ 50%
☐ 70%
☐ 85%

9. Which of the following are tools used by FIs to help prevent and detect internal fraud?

☐ Background Checks
☐ Shared negative files
☐ Analytics
☐ All of the above
10. **Victims are the initial identifiers of more than one in two fraud incidents.**

- [ ] True
- [ ] False
Answers:

Q 1. The correct answer is $18 billion.

Did you Know...
Credit and debit card fraud alone cost FIs nearly $13 billion in 2009, representing 71% of total direct fraud losses.

US Direct Fraud Losses, 2009 (in billions)

$12.8 Card (Credit & Debit)
$2.5 Mortgage
$2 ACH
$1 DDA

Source: IBM Fraud Market Analysis, 2010
More Information

In addition to the direct costs associated with fraud (which include customer refunds, card reissuance, legal expenses, etc.), financial institutions are increasingly paying attention to the indirect costs of fraud. In a recent survey of FIs, respondents ranked “Loss of Productivity” and “Customer Confidence and Reputational Loss” as the top two non-financial losses associated with fraud.

Q 2. The correct answer is 221%.

Did you Know...

Investigations in 2009 uncovered evidence of 143 million stolen records. That’s nearly 400 thousand per day and growing!

Annual Stolen Card Volume, 2009

Source: Verizon and Secret Service 2010 Data Breach Investigations Report
Q 3. The correct answer is **malware**.

**Did you Know...**

When asked to rank the root causes of fraud losses, the financial institution respondents indicated malware as the number one culprit, followed by counterfeit cards and skimming.

**Root Causes of Fraud, Ranked by Severity**

(1-5, where 1 is least severe)

- **Malware**: 3.40
- **Counterfeit cards**: 3.38
- **Skimming**: 3.08
- **Identity theft**: 3.04
- **Account takeover**: 2.92
- **Phishing**: 2.67
- **Social engineering**: 2.52
- **Spoofing**: 2.14
- **Vishing**: 1.95

*Source: Aite Group Survey of 35 North American Banks and Credit Unions, Dec. 2010*
More Information

“Banking Trojans will continue to be the dominant malware in 2011’s threat landscape and this will widely be fueled by the many crimeware kits available on the black market. We’re also observing some collaboration between criminals such as with SpyEye and Zeus, which could very well mean that the sophistication and attack scope can be changed drastically in a short amount of time.”

— Sean-Paul Correll, Panda Security researcher

eWeek Security Watch, January 6, 2011

Q 4. The number of new **checking and savings accounts** opened for the purpose of fraud was higher in 2010 than in any previous year.

Did you Know...

**Fraudulent New Accounts Opened, 2009-2010**

<table>
<thead>
<tr>
<th>New Account Type</th>
<th>2009</th>
<th>2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>New email payment accounts such as PayPal</td>
<td>15%</td>
<td>10%</td>
</tr>
<tr>
<td>New credit card accounts valid only at a specific store</td>
<td>14%</td>
<td>25%</td>
</tr>
<tr>
<td>New checking or savings accounts</td>
<td>11%</td>
<td>15%</td>
</tr>
<tr>
<td>New mobile phone accounts</td>
<td>18%</td>
<td>29%</td>
</tr>
<tr>
<td>New internet accounts such as eBay, Amazon</td>
<td>18%</td>
<td>22%</td>
</tr>
<tr>
<td>New credit card accounts valid everywhere</td>
<td>39%</td>
<td>33%</td>
</tr>
</tbody>
</table>

Source: Javelin Strategy and Research, 2011
Q 5. The correct answer is **False**. ACH fraud resulted in $2 billion in direct losses to financial institutions in 2009, and it is an emerging concern due to aggressively rising loss rates, multiplied by rapid adoption of ACH as a channel for alternative payments.

**More Information**

“Fraud detection is doing what it's supposed to do in existing account fraud, but in new account fraud there's a blind side. Customers can't even check their bank statements to detect it.”

— Jim Van Dyke, president of Javelin

*Bank Info Security, ID Fraud: New Accounts Most at Risk, Feb. 8, 2011*

**Did you Know...**

In response to recent increases in ACH fraud, 40% of financial institutions have invested in new technology solutions to combat it. It is important to note that fraud follows the path of least resistance—so FIs risk being targeted if they fall behind the industry in their ability to detect and manage fraud. Some of the most effective solutions include:

- Account monitoring through data analytics
- Customer direct account monitoring options (such as account alerts)
- In-depth authentication practices
- IP restrictions
- ACH transaction limits
- Predictive modeling
- Payment risk identification
- One-time use card number technology

*Source: ISMG 2010 Faces of Fraud, First Data*
More Information

In 2009, a community bank in the Midwest was victimized by ACH fraudsters that used stolen account credentials to execute 16 unauthorized debit transfers in a single day, for a total withdrawal of $142,000. Fortunately, the accountholder was notified about these transfers by online banking alert e-mails, so 12 of the 16 fraudulent ACH transfers were reversed before the cash could be withdrawn from the fraudsters’ accounts. Total losses from the incident amounted to $35,000—but they could have been much worse if the customer had not opted to receive e-mail alerts.

Q 6. Members of **1.6 million** households reported having at least one bank account compromised, up about 10% over 2009 and the trend shows no signs of stopping. With bank account information, thieves can do anything from clean out the account to change passwords and addresses to order new cards and much more.

**Did you Know...**
A compromised bank account, if not identified quickly, can be the first step to identity fraud which affects 1 in 10 American consumers with a cost of $54 billion to the US economy. While identity fraud theft occurs less often now than it has in nearly a decade, the average financial hit per victim spiked almost 70% from 2009 to 2010 – 631 per person versus $387.

**Average Financial Hit per Victim, 2009 - 2010**

![Average Financial Hit per Victim, 2009 - 2010](chart)

*Source: Mashable.com*
More Information

The “scams of choice” constantly evolve. Proven schemes (such as identity theft) mixed with new information and opportunities lead to off-shoots. Social engineering is one of the latest examples.

“It’s not entirely new, but social engineering attacks – scams that use psychological manipulation to persuade people to divulge sensitive information or to purchase fake antivirus software – will continue to be a threat in 2011,” says Matt Liebowitz, a security specialist for LiveScience. “[It’s] a case of danger in numbers. Those numbers hover somewhere around 500 million, which is the amount of people who use Facebook. Social engineering attacks thrive on Facebook and Twitter because of the enormous pool of potential victims.”

There are various types of social engineering including:
- Phishing: Sending e-mails that appear to come from legitimate businesses to obtain private information
- Vishing: Recreating legitimate-sounding IVR systems that provide a phone number for victims to call in to “verify” account information
- Spoofing: Misleading Internet users to believe they are securely connected to a trusted Web site or receiving e-mail from a specific, trusted source

Source: LiveScience.com, 5 Cyberthreats to Watch For in 2011

Q 7. The answer is False. Skimming – of both ATMs and POS devices – “is the world’s number 1 card-fraud problem,” says Mike Lee, CEO of the ATM industry Association.

Did you Know...

Criminals are increasingly turning to card skimming as a quick and profitable way to steal cash. On average, an ATM skimming attack in the US spans a timeframe of between one and two hours. When you compare that to various estimates of the resulting costs to victims, it’s easy to see the ROI for criminals.

In the US:
- The Secret Service says the crime is responsible for about $350,000 of monetary losses each day in the US.
- Trade group Global ATM Security Alliance estimates that skimming costs the US banking industry about $60 million a year.
- $30,000 per incident is how BankInformationSecurity.com describes the cost.
- BankInformationSecurity.com also notes that ATM skimming attacks cost FIs and their customers 10 times more than losses suffered during robberies.

© 2010 First Data Corporation. All trademarks, service marks and trade names referenced in this material are the property of their respective owners.
And the problem isn't confined to the US:

- The European ATM Security Team reported a 129 percent increase in card skimming incidents in Europe in 2008 over the previous year. A total of 10,302 cases were reported.

Sources: CSOonline.com/International Data Group, BankInformationSecurity.com

More Information

In February of 2011, Toronto police charged five men with 158 criminal charges in connection with an ATM fraud that may have earned the suspects as much as $280,000 from 60 victims since 2009.

Toronto police Det. Phil Hibbeln called it a simple but sophisticated operation. A skimming device — a metal plate-mounted computer chip powered by a small battery — was placed into a bank machine's card receptacle, while an inconspicuous pinhole camera captured customers' PIN numbers. "The PIN data plus the track data was put together and downloaded onto a laptop computer, and that in turn was downloaded onto plastic debit cards," Hibbeln said. The suspects would install the devices before the lunchtime rush, then collect them later in the afternoon.

Sources: ATMSecurity.com, CBC.ca

Q 8. The answer is 70%. Yet, almost half of the most active mobile device users around the world are prepared to pay for goods and services using their phones.

Did you Know...

The financial industry uses added security technology both on the contactless device as well as in the processing network and system to prevent contactless payment fraud, including:

- **Industry standard encryption.** Each contactless device can have its own unique built-in secret "key" which is never transmitted.
- **Authentication.** Issuers have the ability to automatically detect and reject any attempt to use the same transaction information more than once.
- **Confidentiality.** The purchaser’s name is not required to process the transaction – the name isn’t even required to be included in the contactless chip.
• **Control.** The consumer controls the transaction; neither the payment device nor the consumer’s account information needs to be handed over to a clerk during the payment process.

*Source: Near Field Communication World Asia, 2011*

---

### More Information

Can card information be read from a contactless payment device without the consumer’s knowing, allowing the data to be misused? Although it would be extremely difficult to pull off, it’s possible. The industry hasn’t seen fraud of this type, likely due to the security-conscious measures built into the contactless payment process.

- A contactless payment transaction can only occur when the contactless device is held at a very short range – within **two to four inches** – of a capable terminal.
- If a criminal did manage to read the information from a contactless payment device, the security features designed into the device, the payment terminal, and the payment system are in place – just as they are for a magnetic-swipe transaction – to mitigate against the information’s being used for fraudulent transactions.

*Source: Smart Card Alliance*
Q 9. **All of the above.** There are a wide variety of fraud management mechanisms FIs can deploy to combat internal fraud, including background checks, shared negative files and analytics—as well as device fingerprinting, identity verification screening and hot lists.

**Did you Know...**

Internal fraud accounts for an average of 4% of financial institution fraud losses – with many institutions reporting that it constitutes as much as 10% of their fraud losses. Many experts believe that internal fraud is worse than the statistics indicate since employee involvement in a fraud loss is often not recorded or reported. Just as damaging—if not more damaging—are the reputational damage and customer attrition that result when a major internal fraud incident is made public.

**Percentage of Fraud Losses Caused by Fraudulent Employees**

![Graph showing percentages of fraud losses caused by fraudulent employees](source: Aite, Internal Fraud: The Devil Within, 2011)

**More Information**

In 2010, an assistant bank manager at a financial institution in Oregon allegedly stole $1.2 million from dozens of unsuspecting customers. She purportedly began opening additional accounts for existing customers in order to obtain new account commissions, but subsequently began making large unauthorized transfers and withdrawals—mainly targeting sick, disabled and elderly customers. The fraudulent activity was uncovered after complaints of unauthorized transfer activity led to an internal investigation.

*Source: [http://special.registerguard.com](http://special.registerguard.com)*
Q 10. **Victims** detect fraudulent activity, on average, within 52 days of the incident — almost 33 fewer days than other identification methods. The information isn’t surprising to financial institutions: In a recent study, 67% of institutions surveyed say that the most effective way to fight fraud is to make customers aware.

**Did you Know...**

Victims detect fraudulent activity, on average, **within 52 days of the incident – almost 33 fewer days than other identification methods**. The information isn’t surprising to FIs: In a recent study, 67% of institutions surveyed say that the most effective way to fight fraud is to make customers aware.

*Source: 2011 Identity Fraud Survey Report, Javelin*

**More Information**

Your customers are a valuable asset in fraud detection. Help them by providing additional detection tools through education.

- **Go paperless!** Encouraging your customers to go paperless doesn’t just help the environment, it can help reduce fraud. In 2010, more than one in six card fraud victims discovered card fraud by electronically monitoring accounts. FI’s can create statement alerts by flagging or highlighting transactions that might seem suspicious to help customers detect fraudulent activity.
- **Set up a security center in a prominent place on your website.**
- **Teach your customers how to look for the bright green address bar that signals a website has obtained extended-validation SSL certification.**
- **Provide information about consumer identity theft protection services, such as credit monitoring, security alerts, security freezes and data mining services.**

*Source: 2011 Identity Fraud Survey Report, Javelin*