HOW ARE BANKS FIGHTING THE WAR ON FRAUD?

To answer that question, Neustar asked the industry.

neustar

CONTENTS

Neustar sponsored a survey conducted by American Banker of over 230 senior financial executives. All had responsibilities in fraud mitigation or risk assessment. Twenty-percent were from institutions with more than $50 billion in assets, with another 29 percent from businesses whose assets ranged from $1 billion to $50 billion. On some questions, respondents were allowed to select more than one answer.

First, how do you define banking fraud?

As in other industries, financial fraud comes in many flavors.

Three common examples:

- Online transactions with stolen credit card information (card-not-present fraud)
- False information on financial applications
- Account takeovers, where criminals gain full access to financial accounts

Most fraud involves the use of false or anonymous identities. As we'll see, banks are fighting back with tools designed to verify identity or at least raise red flags.

Generally, fraud either directly hurts the banks – when, for example, someone misrepresents themselves on a credit card application – or impacts the customer, as when someone's credit card information is compromised. Indirectly, everyone suffers, often the bank in terms of brand damage.

"Fraud can take on many forms, but in today's environment if it has a negative impact on a company's reputation, its brand or customers, then it is top of mind for financial institutions."

Dorean Kass
Vice President
Neustar

Banks are fighting fraud on many different fronts.

According to banks executives, the top fraud threats are:

52%	Fraud resulting from virus/malware activation
50%	Duplication or skimming of cards
50%	Fraud tied to DDoS attacks
49%	Card-not-present fraud
48%	ACH/wire fraud
47%	Bank customer theft
41%	Account openings and application authentication

Bank executives rank these threats as either high or extremely high. In the latter category alone, card-not-present fraud was ranked the highest at 21 percent.

Who's manning the barricades within the organization?

Responsibility for fighting fraud is fairly widespread:

> **"Banks are struggling with how to get everybody to talk together. You want to be able to see information and patterns shared among all the departments."**

Penny Crosman
Editor in Chief
Bank Technology News
and Technology Editor
American Banker

Smokescreening: Where DDoS meets theft.

In our survey, banks named virus/malware installation and DDoS attacks as two of the top three fraud-related threats. The trend of DDoS smokescreening is one big reason why.

What exactly is smokescreening? While IT and security teams are fully distracted by a DDoS attack, criminals grab and clone private data to siphon off funds, intellectual property and more. In one case, crooks used DDoS to help steal bank customers' credentials and drain $9 million from ATMs in just 48 hours. Such incidents have caused the FDIC to warn about DDoS as "a diversionary tactic."

In fact, in Neustar's 2014 DDoS survey report, 55 percent of DDoS victims (across numerous industries, not just in banking) also lost funds, customer data or intellectual property.

Creating an Emergency to Inflict a Greater One

"Here's an analogy," says Rodney Joffe, Neustar Senior Vice President and Senior Technologist. "When there's a tremendous storm, you run around your house making sure all the windows are closed and you've got the flashlights ready. You're not worried about anything else. DDoS attacks are similar. They create an all-hands-on-deck mentality, which is understandable but sometimes dangerous."

The potential for damage has experts like Joffe worried. "The stakes are much higher," he notes. "If you're a criminal, why mess around with [DDoS] extortion when you can just go ahead and steal – and on a much greater scale?"

Large and small banks rank threats differently.

For instance, card-not-present fraud is named a top threat by:

49% of larger banks

Only **25%** of smaller banks

Larger banks are also more concerned **(49 percent)** about account openings and application verification, along with account takeover **(43 percent).**

One possible explanation for the differences in perception: large banks have more at risk, as well as larger budgets for fraud detection/prevention that better enable them to grasp the severity of threats.

Besides dollar losses, banks worry about the impact on productivity and the customer experience.

Financial executives named these the biggest impacts of fraud:

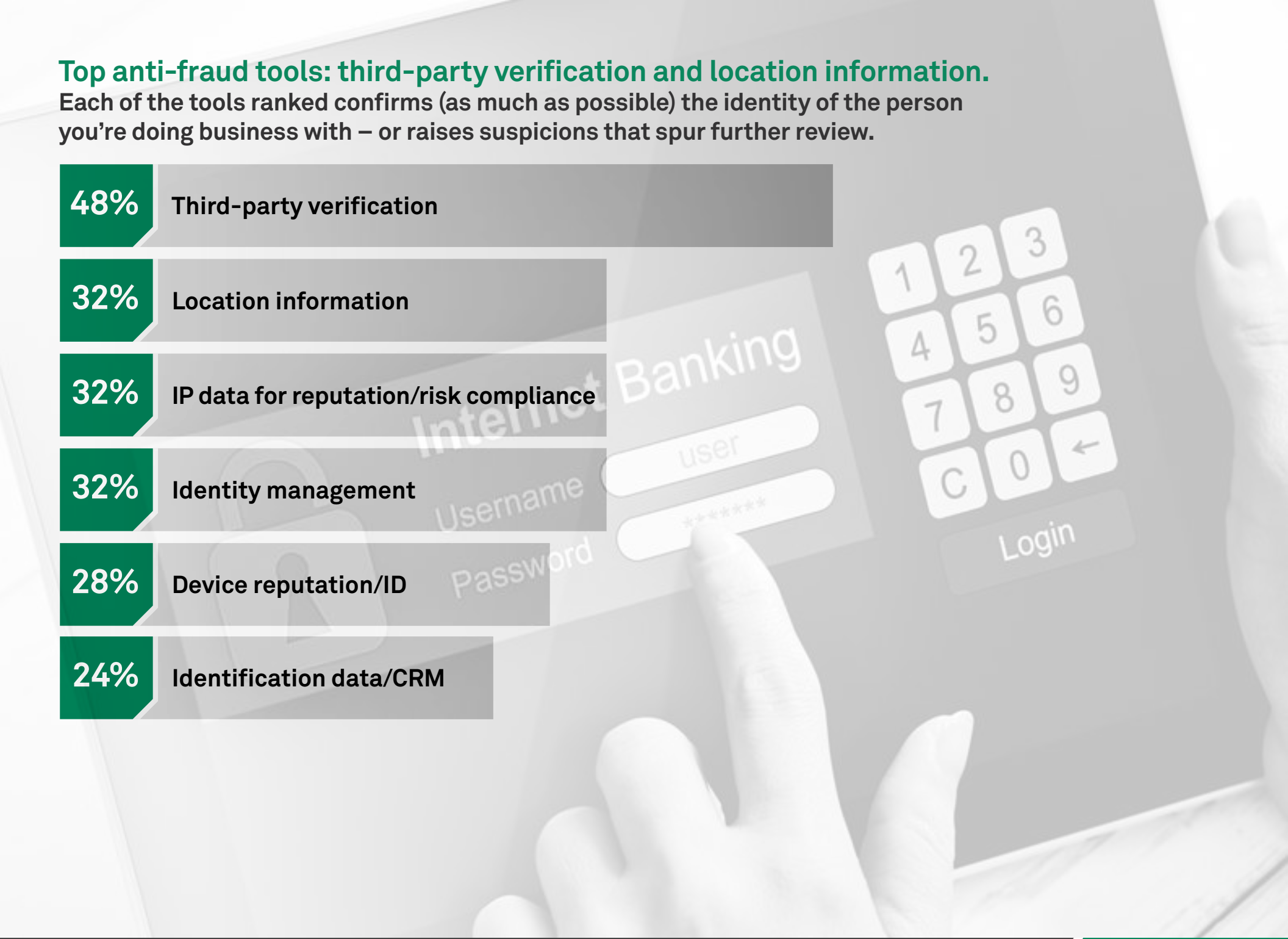
Again, large and small institutions had different points of view. Those citing reputational damage:

- 34% of banks with more than $10 billion in assets
- Only 15% of banks with $1 billion to $10 billion in assets

Top anti-fraud tools: third-party verification and location information.

Each of the tools ranked confirms (as much as possible) the identity of the person you're doing business with – or raises suspicions that spur further review.

- **48%** Third-party verification
- **32%** Location information
- **32%** IP data for reputation/risk compliance
- **32%** Identity management
- **28%** Device reputation/ID
- **24%** Identification data/CRM



What should banks look for in anti-fraud solutions?

Here's a mini-buyer's guide to two of the most popular options.

Third-Party Verification

To scrutinize account openings and authenticate loan or credit card applications, look for verification tools that offer:

Complete Information:
Make sure you get key identifiers like consumer or business name, physical address and phone number – including mobile, landline, VoIP and nonpublic.

Continually updated information:
For example, Neustar updates its database every 15 minutes to ensure accuracy.

Rich mobile data:
Over 30 percent of U.S. households have ditched landline phones for mobile-only, making it harder than ever to match identifiers.

IP Data/Intelligence

To detect fraud by knowing the physical location of a user's device and comparing it with the credit card billing address – or simply to assess the risk associated with an IP address – look for IP tools that feature:

Worldwide IP addresses:
Established providers like Neustar collect and update most of the world's routable IP addresses.

Precise location data:
Be sure the data drills down far enough – not just to country and region/state but also city and postal code, DMA and more.

Network information:
Proxy servers, hosting providers and connection speed and type all give clues to whether the IP address might be used for fraud.

Banks give roughly equal weight to fraud prevention and customer convenience.

Asked to name their top challenge during the next 12 months, more financial executives cite the security-convenience balancing act.

- **67%** Balancing fraud prevention with customer satisfaction
- **42%** Fraud prevention across all banking channels
- **35%** Lack of customer awareness
- **35%** Insufficient budget and/or personnel
- **18%** Difficulty integrating customer data

Achieving the right balance is difficult but important. “When legitimate customers interact with their financial institution, they do not want to have to be asked 15 different ways to identify who they are,” says Dorean Kass, VP, Neustar.

But he also notes that security and convenience can go hand in hand, for instance, with systems that verify phone numbers and device identities silently, behind the scenes.

Risk Tolerance vs. Customer Convenience

On a scale of 1-10, with 1 being very low customer convenience/bank risk tolerance and 10 being the highest, bank executives rated the following activities:

5.6	Card use online
5.5	Card use at an ATM
5.3	Card use at a POS terminal
5.2	Online banking transactions
5.1	Mobile banking
5.0	Online account login
5.0	Mobile app login
5.0	Card-not-present transactions
5.0	Account opening
4.9	Call center identification

With responses ranging only from 4.9 to 5.6, it's clear that banks assign more or less equal importance to security and satisfaction.

Over 30% of banks are increasing investment in fraud prevention.

During the next 12 months banks plan to spend more on:

39%	Dedicated resources
38%	New projects funded
35%	Current projects underway

Among banks reporting greater investments, 85 percent described them as efforts to be proactive, while 59 percent said compliance was the driver.

"Fraudsters have gotten so sophisticated and changed their tactics so quickly that it's hard to keep up."

Penny Crosman
Editor in Chief
Bank Technology News and Technology Editor
American Banker

To summarize, banks are waging war on fraud...

Across all fronts:

Numerous threats mean comprehensive defenses.

With an eye towards lowering losses in key areas:

Especially revenue, productivity and customer satisfaction.

With identity solutions:

Mainly third-party verification solutions and IP/location data.

By balancing excellent customer service with bedrock security:

Generally, banks give the two concerns equal due.

By investing more:

In dedicated resources and both current and new initiatives.

Not surprisingly, larger banks are blazing the trail. As leaders in fraud prevention and cyber-security in general – not only in their industry but throughout global business – major banks are taking no chances. They are aggressively fighting fraud to secure their Internet presence, financial assets, customer experience and brand reputation.

About Neustar Fraud Detection and DDoS Protection

When consumers inquire about your services or attempt online transactions, the more you know about them, the lower your business risk. With real-time verification and IP geolocation services, Neustar accelerates legitimate requests, detects suspicious transactions and substantially lowers fraud. We also offer a flexible array of DDoS mitigation solutions, all backed by our 24/7 response team, some of the best minds in the business. Learn more at **www.neustar.biz.**

About Neustar

Neustar, Inc. (NYSE:NSR) is the first real-time provider of cloud-based information services and data analytics, enabling marketing and IT security professionals to promote and protect their businesses. With a commitment to privacy and neutrality, Neustar operates complex data registries and uses its expertise to deliver actionable, data-driven insights that help clients make high-value business decisions in real time, one customer interaction at a time. More information is available at **www.neustar.biz.**

21575 Ridgetop Circle, Sterling, VA
20166 +1 571 434 5400 / www.neustar.biz

neustar