

## Mobile technology leads to new fraud challenges

Where  
does that QR code  
you shot go?

We  
love our mobiles so much we take much for granted. Would you trust a QR  
code--those funny square symbols--you found on the side of a phone pole?

By Steve Cocheo, executive editor and digital content  
manager

The now very old NY cop show, "The  
Naked City," used to close with the line, "There are eight million stories in  
The Naked City. This has been one of them." Today, Manhattan Island alone is  
home to over 1.5 million people, plus 50.9 million visitors annually. And all  
of them face the risk of being caught up on an identity fraud scam--except for  
the ones perpetrating any one of a number of such crimes.

These numbers come from David  
Szuchman, speaker at ABA's joint Money Laundering Enforcement Conference with  
the American Bar Association, in early November. Szuchman heads up the  
Manhattan (New York County) D.A.'s Office for Cybercrime and Identity Theft Bureau.  
He said his office handles between 200 and 300 new identity theft cases each  
month, most of them arising as a result of arrests by the New York City  
Police Department. The bureau employs not only ten full-time assistant district  
attorneys to handle ID theft and other electronic crime, but also draws on  
additional lawyers, investigators, its own forensic lab, and connections with other enforcement and investigative  
agencies. Cases can involve multiple  
types of crime, ranging from cyber fraud to card and check fraud to money  
laundering, and worse.

Early on, Szuchman told his  
audience of compliance officers, BSA officers, and lawyers that they can rest  
assured that operations like his make much use of Suspicious Activity Reports.

"We use them dozens and dozens of

times every day," said Szuchman.

That may be the last comforting word listeners heard in this session.

ID theft: Gift that keeps on taking

But ID fraud and theft has been a core element in much that the bureau investigates. Szuchman said that even city gangs have found ID theft to be a better business than narcotics trafficking, a former business of choice. As a more-or-less "white collar" crime, the gangs find its less dangerous than their traditional "lines of business," said Szuchman.

"It's less violent," he explained.

The means to acquiring personal data for ID theft ranges widely. Longstanding techniques, such as "skimmers," still see much use. These are handheld devices which steal payment and ID data off magnetic card stripes. Alternatively, criminals may use similar devices designed to overlay card readers on cash machines, capturing data when the user thinks they are accessing the machine.

However, Szuchman noted that newer technologies built off smartphone apps pose more up-to-date threats. He admitted that some new developments "are scaring me," and joked that "no one consults me when they come up with a new piece of technology," regarding the use that bad players might make of it.

The first one he spoke of was Square, the inexpensive plastic dongle device that plugs into a smartphone's audio port and allows card information to be acquired and then transmitted. Square is designed to allow smartphone users to upload this data either as consumers paying for remote mobile purchases or as merchants accepting payment information using their handhelds.

What concerns Szuchman is the risks of such devices for both legitimate use and criminal abuse.

"When Square first started," he said, "they weren't even encrypting the data that was sent over their network. They are now."

Even now, he said, the information necessary to open an account with Square is minimal--an email address, a Social Security number, and a bank account number. Fraud prevention measures are also minimal. Besides the potential for less-protected data to "leak," Szuchman worries about criminals figuring out how to adapt such devices, themselves, as skimming tools to acquire customer data in restaurants and other settings where the customer's card is out of their possession for a time.

Another service that concerns Szuchman is LevelUp, an app that doesn't require even a dongle. Consumers upload credit or debit card information to the service and receive a QR code--those funny square patterns that can be read by smartphones. To other payment devices these are visual representations of the original cards, and Szuchman worries over what could be done with them. He believes the app could facilitate production of the equivalent of counterfeit cards.

"That's the one I have my eyes on," says Szuchman. "It's a game changer, for prosecutors and law enforcement."

#### Smartphone suckers snapping sneaky software

Szuchman expects the challenges to only grow worse. He quoted estimates that there will be 15 billion connected devices by 2015 and that just over half of U.S. cell phone owners now have a smartphone.

There are about as many innovative criminal ideas out there as there are criminals, it would seem. Szuchman's fellow speaker, Michael Benardo, noted that criminals have been bypassing banks themselves, convincing duped consumers to sign up with them directly.

"We have seen criminals selling malicious software for mobile banking, some even falsely displaying bank logos," said Benardo, with the FDIC Cyber Fraud and Financial Crimes Section, in the agency's Division of Risk Management Supervision. Such apps may contain spyware, Benardo said, which allows hackers to use the consumer's own device to access their bank account or payment card data. He advised bankers to tell consumers to stick to mobile banking apps from trusted sites, such as their phone manufacturer, wireless provider, or financial institution.

"Don't download anything financial from 'Bob's App Store'," said Benardo. He also noted that some crooks have been sticking malicious QR codes on telephone poles and other public places, to entice the unwary to snap and click.

"You don't really know where it's taking to you," Benardo warned.

The innovation wheel keeps turning. Benardo said there has been an increase in "smishing"--which is "phishing" for data in SMS texts.

[This article was posted on December 7, 2012, on the website of ABA Banking Journal, [www.ababj.com](http://www.ababj.com), and is copyright 2012 by the American Bankers Association.]