How my bank tracked me to catch a thief

By Jeremy Olshan
Published: Apr 14, 2015 9:47 a.m. ET

Inside the secret ‘signature’ file that banks keep on every customer

I was ordering a kale smoothie from Jamba Juice, when my iPhone buzzed with a text message informing me I’d been robbed.

“Did you make a ATM transaction at 1230 AVE. OF AMERIC NEW YORK NYUS for $303 on March 03 at 1:10 PM. Reply 1 if yes, reply 2 if no,” Citibank C, -0.10% texted, just eight minutes after the crime.

I hadn’t withdrawn $303. I rarely carry cash anymore. But I did use that very same First Republic FRC, -0.75% ATM, one minute before the fraudulent transaction, to withdraw $40 so I could contribute to a gift for a colleague’s new baby.

“2,” I texted back.

“Call Citibank immediately,” came the reply, and before I even got the smoothie I was on the phone with one of the bank’s 1,700 fraud-detection analysts, who suspended my account, opened an investigation into the theft, overnighted me a new debit card, refunded the $303 and told me to change my PIN.

All of this — the fraud, the text-message alert, and the phone call with Citibank — happened in less than 15 minutes. This is the modern world in a nutshell: As we humans loll about, waiting in line for overpriced blended drinks, computers
perform amazing feats of algorithmic gymnastics to make sense of our every ridiculously boring move.

Here’s the far more interesting tale of what happened behind the scenes in Citibank’s computers between the time I left the ATM and the time I got to Jamba Juice, as explained by executives at Citibank and one of the companies behind its software:

When I typed my PIN into the ATM and pushed the button to withdraw $40, the bank’s computer checked my signature. By that I don’t mean the illegible scribbly line I hadn’t even bothered to scrawl on the back of my ATM card. No, this “signature” is a digital John Hancock, a behavioral profile the bank’s software created by crunching the numbers on 13 months of financial activity and distilling all that data into a file one two-thousandth the size, or small enough to check in a few milliseconds. Each transaction is then scored on a scale of riskiness from 1 to 999.

But what is actually in my “signature”?

The software’s “neural network” continuously studies my quirks and idiosyncrasies, learning where, when and how much I spend. This goes beyond noticing when a customer who never leaves Dubuque suddenly goes on a shopping spree in Dubai, said Stu Bradley, senior director of the security intelligence practice for SAS, the company behind software used by Citibank and many other institutions. “It will also learn the way you log in to your online banking and navigate through menu screens.”

My signature, for instance, might include the fact that I use the left shift key on the keyboard to type the capital J in my user name — and that it takes me six seconds to log in, Bradley said. So if I suddenly used the right shift key and took 12 seconds, the software might reasonably wonder if I am really me.

The software has also learned to tell the difference between real human customers and malware banking on stolen account info, which tends to be “more methodical” in its keystrokes, said Bradley.

In my case, the $300 transaction (plus a $3 ATM fee) was probably flagged because of the amount in question, the quick succession of the withdrawals, and perhaps a failed attempt to enter my PIN. Given that this occurred in the busy and touristy Rockefeller Center concourse, it’s also possible the scammer used a skimming device to steal my card information, said Daniel Buttafogo, Citibank’s head of fraud operations for North America.

This is where things get tricky for the computers and the bank. No algorithm is perfect, and in the case of fraud detection many transactions the software finds questionable turn out to be totally legit, forcing banks to weigh just how many “good customers” they are willing to hassle in order to catch one fraudster.

The industry standard is that at least five or six customers need to be inconvenienced to find one fraudulent transaction, said Buttafogo. “If it were an exact science there would be no more fraud at all,” he said. “We are going to impact a lot of good customers, so a big part of this is how best to manage that customer experience.” In other words, banks are searching for a sweet spot between how much they’re willing to annoy their customers and how many fraudulent transactions they’re willing to eat.

The text messages are designed to minimize that inconvenience. Citibank introduced them several years ago for its credit cards but only in the past eight months with debit cards. In some cases the account may be blocked until the customer confirms the legitimacy of the transaction. The banks also compare notes with each other, sharing anonymized versions of this profile data, said Buttafogo. “This is the one area where there isn’t competition among banks.”

I did my part to stamp out fraud just be replying to Citibank’s text before further damage could be done, Buttafogo said. In the bank’s fraud-detection lingo, I “self-serviced.”

In the end, it was reassuring to me that my bank was able to catch the fraud so quickly. And despite all the drama while it was being prepared, the smoothie was delicious.