CIO Monica Eaton-Cardone on Card Fraud: No Signature, No PIN, No Merchant Recourse

Card networks dropped point-of-sale signature requirements last year, yet still do not require a PIN for chip cards. IT exec Monica Eaton-Cardone calls for change as post-EMV rules leave merchants increasingly liable for card fraud and chargebacks.

TAMPA, Fla. (PRWEB) February 25, 2019 -- In 2018, the major U.S. payment card networks dropped their signature requirement for point-of-sale (POS) transactions, in part due to the security capabilities of chip-embedded cards.(1) While the U.S. migration to EMV chip technology was intended to combat fraud, a recent study found that 60 million U.S. cards were compromised between October 2017 and October 2018; of that total, 75% of records were from card-present (CP) transactions, and 90% of those CP cards had EMV chips.(2) Monica Eaton-Cardone, an IT executive specializing in risk management and fraud prevention, believes ongoing card fraud calls for stricter security measures and better protections for merchants, who increasingly bear the costs of fraud.

Though evidence shows EMV has had some success in reducing CP fraud, card-not-present (CNP) fraud has continued to grow. From 2015 to 2016, U.S. CP fraud decreased from $3.68 billion to $2.91 billion while CNP fraud climbed from $3.4 billion to $4.57 billion.(3) The Nilson Report estimated total global card fraud losses to be $24.26 billion in 2017 and projected that by 2022, annual losses will rise to $34.66 billion—including $12.12 billion in the U.S. alone.(4) Juniper Research forecasts that between 2018 and 2023, retailers worldwide will suffer some $130 billion in CNP fraud losses.(5)

In light of these statistics, the 60 million compromised U.S. cards is particularly concerning. Gemini Advisory revealed that 14.2 million of those stolen records resulted from CNP breaches while 45.8 million were from CP transactions, including 41.6 million charges made with EMV-enabled cards.(2) The firm attributes these CP thefts primarily to point-of-sale breaches (think malware and skimmers) and “card sniffing,” or stealing data as it passes over computer networks. Criminals are able to encode the stolen data on magnetic strips on counterfeit cards or use it for online purchases—which means CP data theft can hurt eCommerce retailers who had no fault in the breach.

Eaton-Cardone, who serves as Chief Information Officer (CIO) of Global Risk Technologies and Chief Operating Officer (COO) of Chargebacks911, says that while EMV has the potential to be highly effective at fighting card-present fraud, its execution in the U.S. has fallen short and placed a disproportionate share of the burden on merchants. She notes that chip-enabled cards are only part of the security equation; in other countries, EMV is a “chip-and-PIN” system that requires cardholders to enter their personal code at the point of sale. U.S. banks instead adopted a chip-and-sign protocol; but since they dropped the signature mandate, the risk to merchants has increased. Eaton-Cardone also points out that chip encryption only benefits card-present retailers and has driven many criminals online, contributing to the ongoing rise in CNP fraud that has plagued eCommerce merchants.

“Card networks should have adopted the global-standard PIN requirement as part of the U.S. EMV rollout. With no signature or PIN required, it’s easier for fraudsters to use lost or stolen cards at point-of-sale terminals and harder for retailers to defend against card-present chargebacks,” explained Eaton-Cardone. She also feels eCommerce merchants deserve better protections from fraud. “Not only have online retailers been increasingly targeted by criminal fraud, but they experience far more chargebacks and ‘friendly’ fraud. When it’s a

customer's word against a seller's, banks tend to side with the consumer."

Data compiled by Eaton-Cardone's companies reveal that chargeback stats are growing 20% per year, with friendly fraud increasing 41% every two years. She says that when consumers file unjustified chargebacks for goods they received, retailers are not only out the merchandise and shipping costs, but they must absorb fees of $20 to $100 per transaction—and could face fines of $10,000 and/or lose their card-processing rights if their chargebacks exceed a specified threshold.

"Merchants have a duty to cardholders—and their own bottom line—to implement a multi-layered fraud solution, including chargeback mitigation. However, they should not be saddled with a disproportionate share of the fraud risks, burden of proof or penalties," asserted Eaton-Cardone. "When card networks, issuing and acquiring banks, merchants, and consumers work together to reduce fraud and chargebacks, it will ultimately lead to lower costs and a more sustainable system for all."

Monica Eaton-Cardone frequently discusses fraud prevention, financial technology (FinTech) and security best practices at industry conferences and events. She has been a featured panelist at TRUSTECH, the IATA World Financial Symposium and TRANSACT, and is also available for interviews, panelist opportunities and future speaking engagements. For more information, visit http://monicaec.com.

About Monica Eaton-Cardone:
An acclaimed entrepreneur, speaker and author, Monica Eaton-Cardone is widely recognized as a thought leader in the FinTech industry and a champion of women in technology. She established her entrepreneurial credentials upon selling her first business at the age of 19. When a subsequent eCommerce venture was plagued by revenue-leeching chargebacks and fraud, Eaton-Cardone rose to the challenge by developing a robust solution that combined human insight and agile technology. Today, her innovations are used by thousands of companies worldwide, cementing her reputation as one of the payment industry's foremost experts in risk management, chargeback mitigation and fraud prevention. As CIO of Global Risk Technologies and COO of Chargebacks911, Eaton-Cardone leverages her global platform to educate merchants on best practices in fraud prevention and to spotlight the competitive and economic advantages women can bring to the technology workforce. Her nonprofit organization, Get Paid for Grades, invests in students to inspire a new generation of innovators. Get to know Eaton-Cardone at http://monicaec.com.

1. Sugar, Rachel. "Why Are We Still Signing Credit Card Receipts?"; Vox; December 5, 2018.

2. Alforov, Stas. "Card Fraud on the Rise, Despite National EMV Adoption"; Gemini Advisory blog post; November 5, 2018.

3. Board of Governors of the Federal Reserve System. Changes in U.S. Payments Fraud From 2012 to 2016: Evidence From the Federal Reserve Payments Study; October 2018.

4. "Card Fraud Losses Reach $24.26 Billion"; The Nilson Report; November 2018.

5. Juniper Research. "Retailers to Lose $130Bn Globally in Card-Not-Present Fraud Over the Next 5 Years"; press release issued January 2, 2019.

Contact Information
KJ Helms
JoTo PR
http://www.jotopr.com
727-777-4621

Online Web 2.0 Version
You can read the online version of this press release here.