payments system research briefing

May 2017 | Federal Reserve Bank of Kansas City

Managing Fraud in Remote Payments

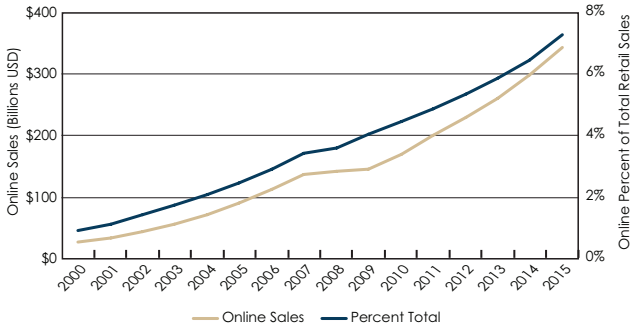
By Zach Markiewicz, payments research specialist, and Richard J. Sullivan, senior economist

Rising e-commerce, telephone, mail order and other remote retail sales—coupled with a technological development to better manage "in-person" debit and credit card payment fraud—have led to an upsurge in card-not-present (CNP) fraud losses in the United States. Merchants and card issuers are at risk as authenticating payment cards and cardholders is more difficult in a remote environment and fraudsters are taking advantage. E-commerce sales alone grew twelvefold from 2000 to 2015, from $27.6 billion to $343.0 billion (Chart 1). Other forms of remote shopping have only added to the number of potentially vulnerable card payments.

Remote sales expanded in part due to payment cards, which allow cardholders to give merchants a card account number rather than the actual card. Indeed, the annual growth rate of remote general purpose card payments was 15.3 percent a year—double the growth of in-person general purpose card payments—for the three-year period ending in 2015 (Federal Reserve System).

Improving payment card authorization for remote payments is an urgent problem because the shift from card-present (CP) fraud to CNP fraud is likely to accelerate. In 2016, many U.S. card issuers added computer chips to their payment cards using Europay-MasterCard-Visa (EMV) standards. These EMV cards are highly secure against counterfeiting and provide the card issuer strong assurance that the card is genuine in a CP environment (Sullivan). As a result, CP fraud from counterfeit cards can be expected to decline as chip cards are rolled out, similar to the experience of other countries that use EMV cards.

Chart 1
Estimated U.S. E-commerce Sales, 2000-15

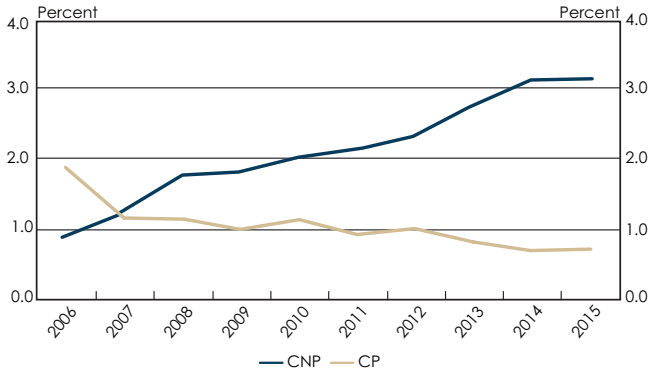


Source: U.S. Census Bureau 2016a, 2016b.
Notes: E-commerce sales are sales of goods and services where the order, price or terms of the sale are negotiated over an internet, mobile device (M-commerce), extranet, Electronic Data Interchange (EDI) network, electronic mail or other comparable online system.

The experience of other EMV countries, however, also suggests card fraud will migrate to purchases through remote channels where CNP transactions are common and where card and cardholder authentication is relatively weak. France is a useful example because its central bank, the Bank of France, has been studying the effect of EMV implementation on CNP fraud since 2002. Rates of payment card fraud in France shifted dramatically away from CP to CNP transactions from 2006 to 2015 (Chart 2). CP fraud declined from just under 2 percent

Chart 2

Shares of Fraudulent CNP and CP Transactions



Sources: Bank of France, various issues and author's calculations.

of CP transactions in 2006 to 0.7 percent of CP transactions in 2015. By contrast, CNP fraud increased from under 1 percent of transactions in 2006 to 3.2 percent of transactions in 2015.

The United Kingdom, Australia and Canada had records similar to France's after they adopted EMV payment cards (Sullivan 2013). Early evidence suggests the same is happening in the United States. One report found that counterfeit card fraud fell 18 percent in the first quarter of 2016, while CNP fraud rose by 12 percent (Auriemma Consulting Group).

The Shift in Fraud Rates Could Be Especially Costly to Merchants

Merchants generally are responsible for all CNP fraud losses—but with the EMV standard in place, merchants who have not upgraded their card readers to accept EMV chip cards also may be responsible for CP fraud. As a result, merchants are working to get up to speed with the EMV standard to avoid CP fraud losses and may not be as focused on the growing threat to CNP transactions. In a recent survey of merchants, 76 percent ranked EMV implementation as their top payment-related challenge while only 15 percent ranked CNP fraud as a top challenge (NRF/Forrester report). Overall, merchants ranked CNP fraud as eighth of 12 options.

Evolution of Methods To Deter CNP Fraud Since 2000

Online merchants have a number of options to deter CNP fraud (Table 1). The most commonly used methods to authenticate a payment card—card verification numbers (CVN) and address verification systems (AVS)—are two of the oldest options.

A CVN, more generally known as the three-digit code on the back of a payment card, specifically helps to secure CNP transactions. CVNs have an added benefit in that they cannot be stored by merchant databases, so they are less vulnerable to breaches than card account numbers.

An AVS deters CNP fraud by matching information the customer provides against the billing address of the card owner. Many CNP fraud perpetrators use a false shipping address to receive products; with AVS, this type of fraudulent behavior is much more likely to be detected and prevented. AVS are also used at self-pay pumps, when consumers are asked to provide their ZIP code before they can begin pumping gas.

Table 1 shows that CVNs and AVS had the highest adoption rates in 2016 (86 percent of respondents to a recent survey of online merchants). Respondents also rated CVN and AVS among the most effective fraud detection tools. Adoption of CVN and AVS increased 10 percentage points from the 2014-15 to the 2016 survey, possibly in anticipation of EMV cards' likely effect on online fraud.

The Future of Remote Authentication in Card Payments

Merchants, card networks and payment service providers are actively researching and developing new and improved card fraud detection tools. Table 1 shows the three fastest-growing tools for fraud detection in 2016 are customer order history, negative lists and postal address validation. These tools grew 32 to 34 percentage points from 2010 to 2016. In addition, merchants increasingly are using services such as Google Maps and internet addresses to investigate the location of the payment and predict potential fraud.

Table 1
Adoption Rates for Fraud Detection Tools Used for Remote Payments

Fraud Detection Tool	2016 percent	2014-15	2012	2011	2010	Percentage change 2010-16
Card verification number (CVN)	86	76	79	75	76	10
Address verification services (AVS)	86	76	77	78	77	9
Customer order history	78	66	43	42	44	34
Negative lists	72	56	38	39	40	32
Postal address validation services	67	52	39	38	34	33
Google Maps lookup	64	47				
IP geolocation	51	42	40	36	27	24
Telephone no. verification/reverse lookup	51	49	22	25	24	27
Order velocity monitoring	51	41	35	38	35	16
Fraud scoring model—company specific	48	37	30	28	28	20
Social networking sites	46	33	10			
Customer website behavior analysis	46	28	22	19	19	27
Positive lists	43	37	20	20	21	22
Shared negative lists—shared hotlist	39	18	17	15	16	23
Multimerchant fraud models	34	14	15	9	12	22
Device fingerprinting	32	22	16	13	9	23
Credit history check	30	10	5	4	5	25
Paid for public records service	25	16	9	14	13	12
Payer authentication (3-D Secure)	23	21	25	23	29	-6
Two-factor phone authentication	13	4				
Biometric indicators	1	1				

Source: CyberSource (Sample sizes: 2016=307, 2014-15=347, 2012=325, 2011=334, 2010=352).

Notes: CyberSource did not publish its survey in 2013. 2014 was combined with 2015 into one publication.

Fraud detection tools aimed at securing remote payments are in early stages of market development and can be clustered into three basic groups: fraud detection modeling, purchase device tracking and biometrics.

Fraud detection modeling includes risk-profiling systems from both in-house and third-party service providers. These systems collect information from various sources to help inform merchants' decisions to approve or not approve a purchase request. Criteria can include all information at a merchant's disposal such as order history, dollar amount of the purchase, merchandise class and public records such as address and telephone number. The use of fraud detection models is growing and is likely to remain a staple for most online retailers.

Purchase device tracking (also called "device fingerprinting"), collects information about a remote computing device used to execute a payment. While only 32 percent of retailers report using device fingerprinting, those that do report it as the "most effective" fraud prevention tool, with fraud detection models a close second (CyberSource 2016). IP geolocation is sometimes categorized with device fingerprinting and is also seen as one of the most effective tools for fraud prevention. However, geolocation is controversial among privacy advocates.

Biometrics is a new class of tools for payment identity management. Biometrics has relatively low awareness and usage but has become more common since the launch in October 2014 of iPhone's Apple Pay service. Apple Pay uses a fingerprint-reading device to authenticate mobile wallet transactions, making it the first major American brand to use biometrics as a payment identification tool. Developers are exploring many new technologies for authenticating payers and their transactions, including eye/retina scanning and facial and

voice recognition. Today, only about 1 percent of merchants report using biometrics to authenticate transactions.

A recent study shows consumers perceive scanning fingerprints and eyes as the most effective forms of payment authentication (Javelin). This is especially true with early adopters of the technology, three-quarters of whom believe fingerprint scanning is either "effective" or "very effective" at authenticating transactions.

The French Experience with 3-D Secure[1]

3-D Secure (3DS) is a protocol that strengthens the remote payment authorization using digital certificates and passwords to authenticate the identity of both customer and payment credentials. The Bank of France, concerned about the rise of CNP fraud following its EMV implementation, sponsored a multiyear project to investigate, inform, and promote strong remote payment authentication.[2]

The Bank of France first encouraged all card issuers to make 3DS a part of all their cardholder services. The Bank of France then conducted a series of consumer surveys to gauge concerns about risk in online shopping. It found that many consumers placed a high value on the security of merchant websites and were more willing to shop at merchants that used strong remote payment authentication such as 3DS to protect online purchases.

Merchants feared customers may abandon remote purchases when prompted for an extra password, but they also needed to consider how customers value secure transactions—over time, customers might adjust to extra steps in a checkout process if it meant greater security.

To investigate online shopping cart abandonment, the Bank of France collected statistics from French online merchants over four years. Its first report found that cart abandonment rates without 3DS were as high as 20 percent; with 3DS, cart abandonment rates were 3 to 4 percentage points higher. But over time, as 3DS became more widely available and the benefits were marketed to consumers, the 3DS abandonment rate converged toward the rate on purchases made without 3DS. In its most recent report, the abandonment rate on 3DS transactions was considerably lower than transactions without 3DS (Bank of France 2016).

Today, a high portion of French remote purchases use strong authentication, and it appears to be paying off. CNP fraud loss rates have declined in France for four years in a row, although CNP losses still account for a disproportionately large share of total fraud losses.

A Fresh Look at 3DS in the United States

In a recent consumer survey in the United States, 80 percent of respondents were willing to provide a CVN for an online purchase. In a companion survey, however, only 57 percent of merchants asked for a CVN (Huen). As a significant majority of consumer respondents appears to prefer strong remote payment authentication, merchants have an opportunity to make security a valued part of their customers' experience.

3DS has been available in the United States since 2001. 3DS is managed by the credit card networks, and the card-issuing bank must subscribe to the service and an online merchant must enable the system on its website. It is the only authentication method in Table 1 whose use declined from 2010 to 2016. It is possible that adoption of 3DS lagged relative to adoption of other authentication methods in the United States because it requires multiple parties to opt-in to the service—i.e., issuers, merchants and consumers all need to participate voluntarily. In France there was at least an explicit encouragement from the Bank of France that the service be offered. Another complicating factor for adoption of 3DS in the United States could be difficulty of offering fair incentives to the various participants. For example, merchants may find it difficult to pin down the fees they must pay card issuers for 3DS or for the costs they may incur to administer the service. Perhaps most critically, the burdensome consumer experience of entering a 3DS password could pose a significant barrier to adoption in the United States.

However, card networks recently announced a significant redesign of the 3DS standard to improve security performance and reduce friction of remote purchases. The protocol provides a uniform experience regardless of the credit card network used in the transaction and regardless of whether the consumer uses a desktop computer or a mobile device.

The service also gives merchants more control over whether to use 3DS on particular transactions. If a merchant has an order from a longstanding customer, for example, and evaluates the

transaction as a low risk for fraud, it can skip 3DS authentication.

Likewise, if the transaction appears to have a high risk of fraud, the merchant can invoke 3DS. The transaction details are sent to the card issuer, who evaluates the transaction and may then choose to skip the password and approve the payment if the transaction is low risk. If the transaction is high risk, the card issuer sends a one-time password to the customer, typically via a mobile phone. A correct passcode from the customer allows the transaction to be completed.

The previous version of the 3DS protocol had a static password the consumer set when he or she enrolled in the system. But customers who did not use 3DS routinely often forgot their passwords. The new protocol ensures that a password is quickly available at the time of purchase. In addition, security is stronger with a one-time password, because it eliminates static passwords that can be a target for hackers.

Still, even a redesigned and streamlined 3DS may not be a good fit for some merchants. A one-time passcode system could be developed by a variety of service providers in the United States other than card issuers or card networks. A likely provider is a merchant acquirer who offers card payment services to merchants. The merchant could add a step in the checkout process of a remote payment to send a unique code generated by the merchant acquirer to the customer's preregistered mobile phone or email address. If the proper code was returned, the merchant could accept the payment. This option is especially valuable for customers that register with a merchant to deter fraud in cases where a fraudster has taken over the cardholder's account.

Conclusions

Difficult questions remain for merchants and policymakers as they look for ways to attenuate what is likely to be a surge toward remote payment fraud after the rollout of EMV payment cards and continued growth in e-commerce. Merchants are reluctant to tighten their payment screening too much to avoid an unacceptable rate of false rejections. Merchants are also wary of increased operational costs associated with manual reviews of high-risk payments, which can take an average of 5 to 15 minutes to investigate.

However, an e-commerce merchant with strong authentication techniques may gain a comparative advantage of increased customer loyalty. And if e-commerce merchants in the United States have outcomes similar to merchants in France, then strong card and cardholder authentication could be expanded without too much dissatisfaction among their customers.

Endnotes

[1]The original version of the 3-D Secure standard is owned by Visa, who allowed other card brands to use the protocol. An updated version of the standard (3-D Secure 2.0) was developed by EMVCo, the standards body for the card brands. EMVCo owns the new standard (http://emvco.com/specifications.aspx?id=299).

[2]By 2007, 100 percent of payment cards in France qualified for 3DS, and 95 percent of French payment terminals were EMV-enabled.

References

Auriemma Consulting Group. 2016. "Counterfeit Credit Card Fraud Reaches Lowest Level Since 2013; Other Fraud Types Increase," July 7.

Bank of France. 2016 and earlier reports. "Annual Report of the Observatory for Payment Card Security."

CyberSource. 2016 and earlier issues. "Annual Fraud Benchmark Report."

Federal Reserve System. 2014. "The 2013 Federal Reserve Payments Study-Recent and Long-Term Trends in the United States: 2000–2012." July.

Huen, David. 2016. "Merchants Aren't Matching Shoppers' Zeal for Security: Report." *Payments Source*, Oct. 27.

Javelin Advisory Services. 2016. "The Future of Cardholder Verification Methods: Beyond Chip and Signature." August.

Kenneally, Steve, and Jane Yao. 2016. "ABA Deposit Account Fraud Survey." American Bankers Association.

Sullivan, Richard J. 2013. "The U.S. Adoption of Computer-Chip Payment Cards: Implications for Payment Fraud." Federal Reserve Bank of Kansas City, *Economic Review*, vol. 98, no. 1, pp. 59-87.

U.S. Census Bureau. 2016a. Estimated Annual U.S. Retail Trade Sales - Total and E-commerce: 1998–2014.

_____. 2016b. "Table 1. Estimated Quarterly U.S. Retail Sales: Total and E-commerce."

payments system research

Website: http://www.kansascityfed.org/research/bankingandpayments/

The Payments System Research Department of the Federal Reserve Bank of Kansas City is responsible for monitoring and analyzing payments system developments. Staff includes:

Terri Bradford
Payments Research Specialist
Terri.R.Bradford@kc.frb.org
816-881-2001

William Todd Mackey
Vice President
William.T.Mackey@kc.frb.org
816-881-2459

Zach Markiewicz
Payments Research Specialist
Zach.Markiewicz@kc.frb.org
816-881-2860

Fumiko Hayashi
Senior Economist
Fumiko.Hayashi@kc.frb.org
816-881-6851

Jesse Leigh Maniff
Payments Research Analyst
Jesse.Maniff@kc.frb.org
816-881-2091

Sabrina Minhas
Research Associate
Sabrina.Minhas@kc.frb.org
816-881-4762

The views expressed in this newsletter are those of the authors and do not necessarily reflect those of the Federal Reserve Bank of Kansas City or the Federal Reserve System.