Electronic Payments: An Analysis of the Rules and Fraud Risks

Information provided in this paper represents the opinions of the author and is intended for informational purposes only. It does not constitute legal advice. If such advice or a legal opinion is required, please consult with competent local counsel.

Electronic Payments: An Analysis of the Rules and Fraud Risks

Jennifer Aguilar
NAFCU Regulatory Compliance Counsel

Today, electronic payments like debit and credit cards are the primary method of choice for consumers. While these types of payment methods make transactions faster, they also make them more susceptible to fraud. The federal regulations and other applicable rules allocate losses to your credit union rather than to the member. This can often leave your credit union holding the bag when someone has gained access to your member's information and conducts fraudulent transactions. As a result, credit unions have a strong interest in detecting and preventing fraudulent transactions. The move toward electronic payments has also given rise to faster check processing through the use of electronic collection and return and recent changes to these laws provide greater incentive to process checks electronically. Further, Same Day ACH has created a near-instant method of processing certain electronic payments and transfers. As consumers continue to demand easier and quicker ways to conduct transactions, payments will only continue to get faster and possibly less secure. Credit unions will need to be prepared to keep up without succumbing to the risks involved.

TABLE OF CONTENTS

INTRODUCTION

Over the past several decades, the way that credit unions and their members conduct business has changed drastically. Credit unions interact with their members primarily through online and mobile banking. Credit unions also interact with each other predominantly through electronic means. Members who previously made payments with cash are now making those payments with debit or credit cards. Online shopping has taken over. Even paper checks are now processed electronically and ACH transactions can be processed the same day they were initiated. Demand for faster and more convenient payments is driving the race for new payment technologies.

It is important to understand how these trends away from paper and face-to-face interactions can impact a credit union – not only in how it interacts with its members and other financial institutions, but also how its regulatory and contractual responsibilities interplay with this trend. Fraud continues to be a supervisory priority for NCUA, so Regulation E's and Regulation Z's unauthorized use response requirements are under scrutiny. From a safety and soundness perspective, mitigating losses from fraudulent transactions is essential. Additionally, the compliance deadline for the recent changes to Regulation CC will be here before you know it and Phase 3 of Same Day ACH has arrived.

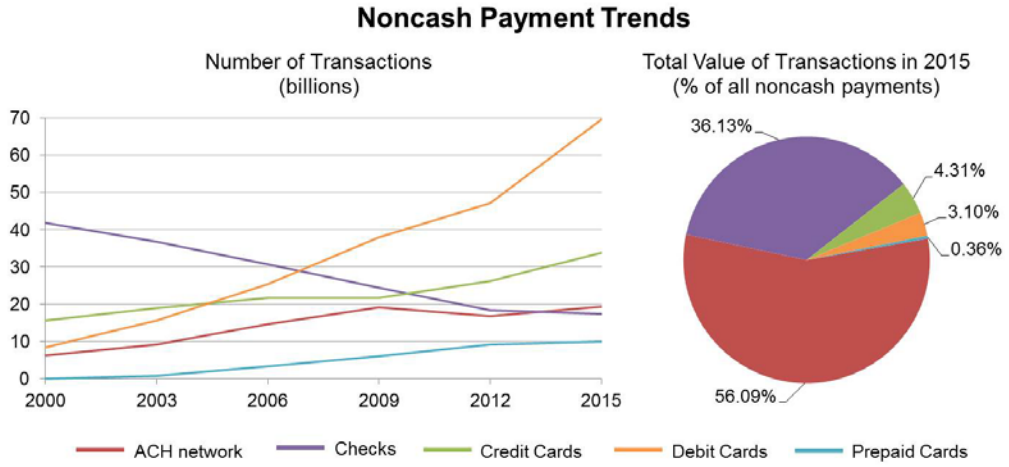
THE RISE OF THE ELECTRONIC PAYMENTS

In 2000, the Federal Reserve conducted its first study on how payments are made in the United States. The Retail Payments Research Project focused exclusively on noncash payments – checks and electronic payments. The first research project compiled data on the number of noncash transactions as well as the total dollar value of these transactions. These data were further broken down into numerous subcategories. For example, check data were collected on the payer, payee and purpose; electronic transaction data were collected on debit cards, credit cards and ACH transactions. The results were compiled to give industry a snapshot on how noncash payments are made and the scope of electronic payment use. This initial research project has turned into a comprehensive Payments Study (Study) that the Federal Reserve conducts every three years. A targeted annual Supplementary Study (Supplementary Study) was also conducted in 2017. For ease of comparison across multiple studies, ACH on-us data is omitted from all calculations in this article, as this data has only been collected since 2012. Some of the previous data were revised as part of the Supplementary Study; the revised data is included in this article and presented as 2016 data.

Noncash Payment Trends

While it is no surprise that the number of noncash payments has grown significantly over the past seventeen years, it is useful to dig into some of the data to understand how consumers and businesses are using the various types of noncash payments. In 2000, over half of all noncash payments were made with checks, both in number and value. While the check payer (person making the payment) was split nearly evenly between consumers and businesses, business payers accounted for 62% of check value. By 2015, checks accounted for only 12% of the number of noncash transactions. Consumer payers continued to account for about half of the number of checks, however, business payers continue to dominate check value, accounting for 80% of check value in 2015.

The total number of all electronic payments first surpassed the total number of checks in 2003, but it was not until 2009 when the total value of all electronic payments surpassed the total value of checks. Currently, ACH network transactions are the only individual type of electronic payment that surpasses checks in both number and value. The number of ACH transactions has more than tripled since 2000. This increase can be attributed, in part, to the increased use of electronic checks – paper checks that are written but later converted to electronic payments are included in the ACH transaction data. Over 2 billion checks were converted to ACH transactions in 2015, compared to only 300 million in 2003. The value of ACH transactions has also grown significantly – from $18.6 trillion in 2000 to $41.6 trillion in 2015. These transactions accounted for almost 90% of the value of all electronic payments in 2015.



Card Trends

Debit cards are currently the most used type of noncash payment. There were 73.8 billion debit card transactions in 2016. Only 8.6 billion transactions were made with a debit card in 2000. That is an increase of over 700%. This rapid increase, along with the decline in checks, indicates the overall replacement of checks by debit card transactions. Consumers today are more likely to make point-of-sale purchases using a debit card, whereas consumers used to make these purchases with a check or cash.

Overall, credit card use increased between 2000 and 2016 but not nearly as much as other types of electronic payments. The overall modest growth in credit card use is due in part to the financial crisis that began in 2008. Between 2000 and 2003, the number of credit card transactions grew an average of 6.7% per year and the total value of credit card transactions increased nearly 10% per year. This growth continued between 2003 and 2006, but at a slower rate. By 2006, credit card use began to decline. From 2006 to 2009, the number of transactions declined 0.2% each year and the total value of transactions declined 3.4% each year. Credit card use has again been on the rise since 2009. In 2016, there were 37.8 billion credit card transactions for a total value of $3.3 trillion.

Prepaid card use is also on the rise. In 2003, there were 800 million prepaid card transactions. Between 2006 and 2009, prepaid cards were the fastest growing type of noncash payment in both number and value – growing an average of 21.5% and 22.9% per year, respectively. This rapid growth continued between 2009 and 2012, however, growth has slowed significantly since then. In 2016, there were 10.7 billion prepaid card transactions for a total value of $290 billion. Although the use of prepaid cards has expanded rapidly over the past several years, prepaid cards remain the least used among all types of noncash payments.

Despite the increased use of debit cards, credit cards and prepaid cards, card transactions continue to account for only a small percentage of the total value of all noncash payments. Together these accounted for nearly 74% of the number of noncash payments but only 8% of the total value of noncash payments in 2015. This small share of total value has to do with the average value of card transactions compared to the average value of ACH transactions and checks. In 2015, the average value of a card transaction was only $55, while the average value of an ACH transaction was $2,159 and the average value of a check was $1,554.

The relatively small values of card transactions can be explained in part by the differences between how consumers and businesses use noncash payments. Debit cards are, by far, the preferred method of payment for consumers. As previously discussed, debit cards have largely replaced small dollar consumer check and cash transactions. Consumers continue to use checks and ACH transactions to make large dollar transactions such as rent and mortgage payments. In each month of 2015, consumer households made an average of 45 debit cards transactions, 19 credit cards transactions, 7 ACH transactions and 7 checks. This is a substantial change from 2000 when consumer households made an average of 7 debit card transactions, 12 credit card transactions, 2 ACH transactions and 19 checks per month.

Businesses predominately use checks and ACH transactions. Until 2012, checks were the most used type of noncash payments by businesses. By 2015, businesses made more ACH transactions than checks. ACH transactions are continually used for large dollar transactions such as payroll and payments to other businesses. Checks remain the second most used type of noncash payment for businesses. Business card use has increased but not nearly as rapidly as consumer card use. In 2015, business made just over 7 billion card transactions whereas consumers made 96 billion card transactions.

Noncash Payments Over Time

	2003			2009			2015		
	Number	Value	Average	Number	Value	Average	Number	Value	Average
Total Noncash Payments	81.2	66.7	822	109	72.2	663	139.9	74.2	654
Credit Cards	19	1.7	89	21.6	1.9	89	33.8	3.2	93
Debit Cards	15.6	0.6	40	37.9	1.4	38	59.6	2.3	38
Prepaid Cards	0.8	0.02	26	6	0.14	24	9.9	0.3	27
ACH Transactions	6.2	18.6	2,989	19.1	37.2	1,947	19.3	41.6	2,159
Checks	36.7	39.3	1,070	24.5	31.6	1,292	17.3	26.8	1,554
Numbers in billions, Value in $ trillions									

The steady rise of electronic payments will only continue in the coming years. Especially as new payment technologies are developed, credit unions can expect consumers to rely less and less on checks and cash – though there is no indication that these payment methods will disappear anytime soon. As credit unions continue to see more electronic payments, they also continue be on the lookout for the unique risks these payments pose.

RECENT TRENDS IN FRAUDULENT TRANSACTIONS

Beginning in 2012, the Payments Study incorporated data on unauthorized use and various fraud types. The 2012 Study estimated that 32.3 million unauthorized transactions

were made in 2012, the vast majority of which came from unauthorized use of a card. Institutions reported 29.8 million unauthorized card transactions. Cards tend to have a much higher fraud risk because they are used irregularly at a number of different merchants, while ACH transactions and checks are predominately used for regular payments where the fraud risk is rather low, such as rent and payroll. The 2012 Study also found that the number of unauthorized transactions where the card was not present was much higher than the number of unauthorized card-present transactions. However, the average value of unauthorized card-present transactions was much higher than the average value of card-not-present transactions.

ACH and check fraud accounted for a much smaller portion of the total number of unauthorized transactions in 2012. Institutions reported 1.7 million unauthorized ACH transactions and only 900,000 unauthorized checks. While the overall number of unauthorized ACH transactions and checks was much lower than the number of unauthorized card transactions, unauthorized ACH transactions and checks tended to have a much higher value than unauthorized card transactions. The average value of unauthorized ACH transactions and checks was $736 and $1,272 respectively. On the other hand, the average value of unauthorized credit and debit transactions was only $136 and $104, respectively.

The 2015 Study looked at various fraud types and fraud channels for card transactions. It found that counterfeit cards were the most common type of card fraud, followed by fraudulent use of an account number. In-person fraud versus remote fraud was split rather evenly in 2015 – 54% to 46%, respectively. This split corresponds to the current trend in fraud type. Counterfeit card fraud, a form of in-person fraud, accounted for 44% of all card fraud. Fraudulent use of an account number, a form of remote fraud, accounted for 39% of all card fraud. The 2015 Study also found that remote transactions tended to have a higher average value than in-person transactions. This is a reversal from 2012 where card-present transactions had a higher average value than card-not-present transactions.

Chip-enabled cards are expected to decrease card fraud, especially counterfeit card fraud as chip technology makes it more difficult to create counterfeit cards, but it will be some time before there is a noticeable drop in counterfeit fraud rates. Chip technology is still in the infant stages in the United States. Only 20% of all cards are chip-enabled and most of these cards continue to have a magnetic strip. Merchants have also been slow to transition to chip technology. The 2015 Study estimated that only 2% of all in-person card

transactions in 2015 were made with a chip. While chip technology may cut down on in-person fraud, it will not eliminate card fraud. In countries with widespread use of chip technology, remote fraud is occurring at much higher rates than in the United States. For example, 97% of in-person card transactions were made with a chip in Europe. In the United Kingdom and France, nearly 70% of all unauthorized card transactions were made via remote fraud.

The Supplementary Study revealed that chip technology is growing quickly in the United States – 19% of all in-person card payments in 2016 were made using chips. As suspected in the 2015 Study, this expansion of chip technology has led to a rise in remote card fraud. Remote fraud increased from 46 % in 2015 to 59% in 2016. As predicted, this increase was primarily due to the decline in counterfeit card fraud, which dropped to 36%. This trend is expected to continue in the coming years.

While electronic payments offer improved speed, efficiency and ease of use, the threat of fraud surrounding electronic payments continues to present a tremendous risk to credit unions. As cash continues to fade away and electronic payments become more and more prominent, managing that risk will only become more critical for the industry.

UNAUTHORIZED USE AND LIABILITY

While the transition to electronic payments has generally been a positive experience, electronic payments are more susceptible to unauthorized use. As discussed in the Payments Study, millions of unauthorized transactions occur every year. While the method of how fraud is being conducted has been changing from in-person fraud to remote fraud, there has been no indication that fraud is declining. Fraudulent transactions pose a threat to both your members and your bottom line; this likely explains why fraud remains a NCUA supervisory priority.

Since the consumer regulations significantly limit a member's liability for fraudulent transactions, the credit union is ultimately responsible for fraud losses. As a result, unauthorized use continues to be a concern among credit unions. Both Regulations E and Z have specific procedures in place that credit unions must follow when members inform them of an unauthorized transaction. Regulation E's provisions apply to all electronic fund transfers (EFTs), such as debit card and ACH transactions. Regulation Z's provisions apply to open-end credit accounts, such as credit cards and HELOCs. Regulations E and Z apply only to accounts that are used primarily for personal, family or household

purposes, meaning business accounts are generally excluded. In addition, Visa and Mastercard have their own liability provisions, which are also discussed briefly.

Regulation E

As a starting point, it is important to understand what types of transactions are considered "unauthorized" under Regulation E's rules. An unauthorized EFT is defined as any EFT from an account initiated by someone without authority to initiate the transfer and from which the member receives no benefit. Unauthorized use includes a transfer using an access device, such as a card, that was obtained by robbery or fraud.

This definition contains a number of important limitations. First, consider the scenario where your member gives her debit card to her son to buy groceries and the son buys a new television instead. The television purchase is not necessarily an unauthorized transaction. Under the definition, when a third party is given authority to make transactions, the member is liable for all transactions, even those that exceed the scope of authority, unless she notifies the credit union that the third party no longer has the authority to make transactions. Second, suppose your member can never seem to remember his PIN so he writes it on his debit card. His card is stolen and used at an ATM. If the member timely notifies the credit union of the unauthorized ATM transaction, his negligence cannot be considered in determining the amount of his liability. Finally, think of when a member purchases merchandise and is later dissatisfied with the purchase or the merchandise is defective. That purchase is not an unauthorized transaction under Regulation E because it was initiated by the member.

Regulation E's error resolution procedures are triggered when the member notifies the credit union that an unauthorized EFT has occurred. The member has sixty days from the date the credit union sent the periodic statement that reflects the unauthorized EFT to make such notification. The notification must include information sufficient for the credit union to identify the member, account number and unauthorized EFT. Oral notification from the member is sufficient to trigger the error resolution procedures. Credit unions may require members to provide written confirmation of an unauthorized EFT within ten days of an oral notice, but the timing requirements would still be based on the date the credit union received the oral notice.

Once it has received notice of an unauthorized EFT, a credit union has ten days to investigate and determine whether an unauthorized transaction has occurred. When the alleged unauthorized EFT involves a transaction at a point-of-sale terminal, the

commentary explains that the investigation must include verifying the information transmitted as part of the transaction. For example, the credit union may request a sales receipt to verify the amount of the transaction. When the alleged unauthorized EFT involves a transaction with a third party and the credit union does not have an EFT agreement with that third party, a review of just the credit union's own records satisfies the investigation requirement. Exactly what internal records must be reviewed will depend on the facts and circumstances involved. Some records that may be reviewed include payment instructions, transaction records, account history and location of the transaction relative to the member's location or usual transaction area.

After completing the investigation, a credit union has three business days to notify the member of its determination. If the credit union determines that an unauthorized EFT occurred, the credit union has one business day after making such determination to correct the EFT. If the credit union determines that no unauthorized EFT occurred, the rule requires the credit union to provide the member with a written explanation of its findings and inform the member of his or her right to request documentation supporting that finding. Documentation must be provided promptly upon such a request.

The ten day timeframe can be extended if the credit union meets certain criteria. A credit union may take up to forty-five days to complete its initial investigation if the credit union does all of the following:

- Provisionally credits the member's account in the amount of the alleged unauthorized EFT within ten days of receiving notice from the member;
- Informs the member of the amount and date of the provisional credit within two days of making such credit;
- Allows the member full use of the credited funds;
- Corrects any EFT within one business day of determining it was unauthorized; and
- Reports the results of the investigation to the member within three business days of completing the investigation.

If a credit union requires written confirmation of an oral notice and does not receive that written confirmation within ten days of the oral notice, the credit union does not have to provide the provisional credit. If a credit union complies with the liability provisions contained in section 1005.6, discussed below, the credit union may withhold a maximum

of $50 from the provisional credit. If a credit union determines that the EFT was not unauthorized, the member must be notified of the following when the credit union debits the provisional credit: (1) the date of the debit; (2) the amount of the debit and (3) that the credit union will honor, without charge, all payments from the account within five days of the notification as long as those payments would have been covered but for the debit.

The forty-five-day timeframe may also be extended in certain situations. A ninety-day timeframe applies when the EFT at issue was a point-of-sale debit card transaction. This includes all debit card transactions made at a merchants' point-of-sale terminal, including cash-only, mail and telephone transactions. A ninety-day timeframe also applies when the EFT was not initiated in a state. A special timeframe applies when the EFT at issue was made within thirty days after the first deposit to the account. In that case, the original ten day timeframe is automatically extended to twenty days and the forty-five-day timeframe is automatically extended to ninety days.

In addition to the error resolution requirements, Regulation E also has a liability provision for unauthorized EFTs. Under section 1005.6, members may be held liable for unauthorized EFTs only if the credit union has disclosed to the member a summary of his or her liability for an unauthorized EFT, the telephone number and address where a member may notify the credit union of an unauthorized EFT and the credit union's business days. If an access device was used as part of the unauthorized EFT, two additional conditions apply: it must be an accepted access device and the credit union must have provided a way to identify the member to whom the device was issued, such as a PIN or signature comparison. According to the commentary, credit unions do not have to provide separate means of identification for each user when multiple access devices are issued for the same account.

If these conditions have been met, a credit union may impose liability on the member for an unauthorized EFT or a series of related unauthorized EFTs. The amount of liability depends on when the member notifies the credit union that an unauthorized EFT has occurred. Notice may be provided orally or in writing. Under the rule, notice is given when the member takes reasonable steps to provide the credit union with pertinent information, regardless of whether the credit union actually receives such notice. Where the credit union has disclosed a specific telephone number or address for members to provide notification of an unauthorized EFT and the member provides notification at a different number or address, the credit union is still considered to have received the

notice. Notice by a third party acting on the member's behalf is also sufficient; as is constructive notice, where the credit union on its own learns of information sufficient to lead to a reasonable belief that an unauthorized EFT has occurred.

The timeframes for providing notice depend on whether or not an access device was used. If an access device has been lost or stolen, the member has two business days from the date he or she learns of the loss or theft of the access device to notify the credit union. If the member does so, liability is limited to the lesser of $50 or the amount of the unauthorized EFTs. The day the member learns of the loss or theft does not count towards the two days. The commentary provides the following two examples to help clarify the timeframe:

Member learns of loss or theft on Wednesday.	Member has until midnight on Friday to inform the credit union.

See, 12 C.F.R. Part 1005, Supp I, Comment 6(b)(1)-1.

Member learns of loss or theft on Friday.	Member has until midnight on Monday to inform the credit union.*

*Assuming Saturday is a business day for the credit union
See, 12 C.F.R. Part 1005, Supp I, Comment 6(b)(1)-3.

If the member does not inform the credit union within two business days then the member's liability increases. The member's liability will be the lesser of $500 or the result of the following calculation: (1) the lesser of $50 or the amount of the unauthorized EFTs conducted in the first two days plus (2) the amount of all unauthorized EFTs that occurred after the end of the second business day but before the member provided notice. Again, the commentary provides some helpful examples:

Monday	Tuesday	Thursday	Friday	
Member's card is stolen. Member learns of the theft.	$100 unauthorized EFT is made.	$600 unauthorized EFT is made.	Member informs credit union of the theft.	Member is liable for $500 because this is less than the calculation ($50 for the first two days plus $600 for transactions after two days but before notice).

Monday	Tuesday	Thursday	Friday	
Member's card is stolen. Member learns of the theft.	$600 unauthorized EFT is made.	$100 unauthorized EFT is made.	Member informs credit union of the theft.	Member is liable for $150 because the calculation ($50 for the first two days plus $100 for after two days but before notice) is less than $500.

Members may also be liable for additional amounts in certain situations. Members have sixty days from the date the credit union sends the periodic statement reflecting an

unauthorized EFT to notify the credit union of the unauthorized EFT. If a member fails to provide notice within sixty days, the member is liable for all unauthorized EFTs that occur after sixty days and before notification, as long as the credit union can show that these transactions would not have occurred if the member had provided notice within the sixty-day timeframe. When a lost or stolen access device is used, liability for unauthorized EFTs occurring before a periodic statement is sent and within the following sixty days is included in the $50 and $500 limits discussed above. If state law or an agreement provides lower liability limits, these limits will apply instead of those provided in Regulation E.

If a lost or stolen access device was not used, the member has sixty days from the date the credit union sent the periodic statement that reflects the unauthorized EFT to provide notification. The liability limits based on periodic statements discussed in the preceding paragraph apply, but the $50 and $500 limits do not apply. Unfortunately, neither the regulation nor the commentary specifically discusses unauthorized EFTs where an access device was used but not because it was lost or stolen, such as a counterfeit or cloned card. A strict reading of the regulation seems to indicate these transactions would be treated as if an access device was not used because the regulation specifically references only lost and stolen cards. However, the commentary to the access-device-not-used rule specifically references only transactions where no access device was used at all. In the absence of specific guidance, it will be up to the credit union to determine how to treat these types of transactions. In either case, Regulation E limits the amount credit unions may recover from the member when an unauthorized EFT occurs.

Regulation Z

The error resolution procedures discussed below apply to all open-end credit plans. That is, credit extended under a plan where the credit union expects multiple transactions, imposes a finance charge on the outstanding balance and replenishes available credit as outstanding balances are repaid. Among other products, this can include credit card plans, unsecured lines of credit and home-equity lines of credit.

The error resolution provision under Regulation Z applies to all "billing errors." A billing error includes transactions that are not made by a member or by someone with authority to use the credit. A billing error also includes transactions where the goods or services involved are not accepted by the member or are not delivered as agreed. This covers situations where the member refused delivery, the goods or services were different from

what was ordered, the wrong quantity was delivered or the delivery was late. A billing error does not include disputes related to the quality of goods or services the member accepted.

Regulation Z's error resolution procedures are triggered when the member notifies the credit union that a billing error has occurred. This notice must be written and must be received within sixty days from the date the credit union first sent the periodic statement reflecting the error. The notice must also include sufficient information for the credit union to identify the member and account number, describe why the member believes there is an error and the type, date and amount of the error. The rule requires credit unions to send a written acknowledgment to the member within thirty days of receiving this notification, unless the credit union completes the error resolution process within that thirty-day period.

A credit union has two complete billing cycles, not to exceed ninety days, from the date it receives the notice to investigate and resolve the error. The billing cycle in which the credit union receives the notice does not count toward the two cycles. While an investigation is usually conducted, credit unions may elect to correct an error without an investigation or determination that the error actually occurred. If a credit union determines that an error occurred as described in the notice, the rule requires it to correct the error, including any finance or other charges, and send a correction notice to the member. The rules do not provide specific content requirements for the correction notice; the notice only needs to sufficiently describe the correction. The correction notice may be provided on its own or with a periodic statement.

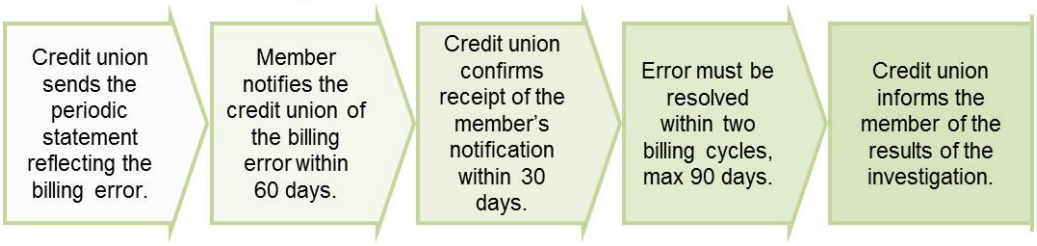
If a credit union determines that an error did not occur, the rule requires it to send a notice to the member that explains the credit union's determination. If a credit union determines that a different error has occurred, the rule requires the credit union to send the explanation notice and correct the error. The rule also requires credit unions to provide evidence supporting its determination if the member requests. A reasonable investigation must be conducted before a credit union can determine that no error or a different error has occurred.

During and after the error resolution process, a number of additional rules apply. During the process, members may withhold any portion of a periodic payment, including finance or other charges, relating to the disputed amount. Credit unions are prohibited from collecting any withheld amount, making any adverse report to credit reporting agencies

based on the member's nonpayment of a disputed amount and accelerating or restricting the member's account. After the process, if a credit union determines that the member owes any amount then it must provide written notice to the member of the amount due and the due date and allow any disclosed time periods to lapse before imposing an additional finance charge. If the amount is still unpaid and at least ten days have passed since the due date, a credit union may report the account as delinquent, unless the member notifies the credit union that the amount is still in dispute.

When a credit union learns additional information after the conclusion of the error resolution process, special rules apply. According to the commentary, if a credit union later discovers that no error actually occurred, it cannot reverse a credit that it has already given to the member. However, a credit union may reverse a credit if the member receives credit from another source for the same error. For example, if a member receives a refund from the credit union and a merchant for the same purchase, a credit union may reverse its credit as long as the amount the member retains is equal to the full amount of the error.

Regulation Z's Error Resolution Process



Additional Rules for Credit Cards

Regulation Z also has a liability provision for unauthorized use of a credit card. For purposes of this provision, unauthorized use is any credit card transaction by someone without authority to use the card and from which the cardholder receives no benefit. The cardholder may be liable only if the credit card is an accepted credit card, the credit union has provided a way to identify the cardholder or authorized user, and the credit union has disclosed the member's potential liability and how the member may inform the credit union of an unauthorized transaction. Means of identification may include a signature or photograph on the card; but a magnetic strip alone is not a sufficient means of identification.

Since one of the conditions to imposing liability is that the credit union provide a way to identify the cardholder, the commentary explains that members may not be held liable

for unauthorized transactions where the card was not presented if no other identifying information was collected at the time of the transaction. Any information that appears on the card itself is not sufficient identifying information. This means that a credit union cannot rely on an expiration date or card identification number as identifying information. This particular limitation is especially important as we continue to see a rise in remote card fraud so credit unions may need to ensure they are providing a means to identify the cardholder for remote transactions.

If these conditions have been met, a member's liability is limited to the lesser of $50 or the amount of unauthorized transactions occurring prior to the member notifying the credit union of the unauthorized transactions. When a credit union seeks to impose any liability on the member, an investigation is required. The investigation must be reasonable but the exact scope of the investigation will depend on the facts and circumstances involved. Credit unions may request the member's assistance in conducting its investigation but cannot rely solely on the member's failure to do so as a reason to deny the claim. Some steps in a reasonable investigation may include reviewing account history, comparing the address where goods were delivered to the member's residence or work address, comparing the signature on the receipt to a signature the credit union has on file or requesting a copy of a police report.

When it comes to how a member must provide notice of an unauthorized credit card transaction, the rule is rather flexible. There are no specific timeframes for when notice must be provided and notice may be provided orally or in writing. Under the rule, notice is given when the member takes reasonable steps to provide the credit union with pertinent information about the unauthorized transactions, regardless of whether the credit union actually receives such notice. Where the credit union has disclosed a specific telephone number or address for members to provide such notification and the member provides notification at a different number or address, the credit union is still considered to have received the notice. Notice by someone other than the cardholder is also sufficient. If state law or an agreement, including a Visa or Mastercard agreement, provides lower liability limits, these limits will apply instead of those provided in Regulation Z.

Card Network Rules

When a credit union joins a card network, it generally contractually agrees to abide by the rules of that network. When these rules provide greater protections to cardholders regarding liability for unauthorized use, these protections will apply instead of those

outlined in Regulations E and Z. If your credit union has joined one of these networks, it is important to be as familiar with their rules as with the federal regulations. While this section highlights some of the protections in the card network rules, the rules discussed below may not apply to your credit union. These rules are governed exclusively by contract so the credit union will want to review the agreement it has with its network and reach out to its network representative with any specific questions or concerns.

Over the past few years, several card networks have moved toward a zero liability rule for unauthorized use. As a result, when a transaction falls within the scope of these rules, a credit union cannot rely on Regulation E or Regulation Z to impose some liability on the cardholder. Exactly what constitutes unauthorized use will depend on the particular card network. The timing requirements for notice, investigations and refunds also vary by network.

For example, the Visa Rules explain that a credit union must generally limit liability to $0 when a cardholder notifies the credit union of an unauthorized transaction. When a Visa debit card is involved, the rules require a credit union to provide a provisional credit in the amount of the unauthorized transaction within five days of receiving notification from the cardholder. The Visa Rules do not provide a specific timeframe for when a cardholder must notify the credit union of an unauthorized transaction so a credit union may be required to credit an account under the Visa Rules even when the Regulation E timeframes have expired. If the credit union believes that additional investigation is needed, it does not have to provide the provisional credit within this timeframe. In that case, the Visa Rules defer to the applicable regulation.

The Visa Rules also provide a narrow exception to the zero liability rule: liability may be imposed if the credit union determines that the cardholder was negligent or acted fraudulently. The credit union must have "substantial evidence" of such acts. When the cardholder acted negligently, the Visa Rules allow a credit union to increase her liability, but this liability still cannot exceed the applicable Regulation E or Regulation Z liability limitations. Whether a cardholder acted negligently will generally be determined by state law, so a credit union may need to work with an attorney or its Visa representative when dealing a potentially negligent cardholder.

Maximum Liability for Unauthorized Transactions

	Debit Card	Credit Card
Member properly informs credit union of unauthorized transaction	$0	$0
Member is found negligent	$50, if the member informs the credit union within two days	$50
	$500, if the member informs the credit union after two days	
Member acted fraudulently	Potentially unlimited liability	Potentially unlimited liability

As noted above, certain scenarios are not covered under Regulation E's or Regulation Z's error resolution processes, such as when the cardholder is dissatisfied with a purchase. However, these scenarios may be covered under the card network rules. Under the chargeback rules, a cardholder may be able to dispute these types of transactions. The chargeback rules generally apply when the cardholder made the transaction but something has gone wrong. They generally do not apply to transactions that were not made by the cardholder or an authorized user. For example, under Mastercard's Chargeback Guide (Guide), here are some scenarios that are covered:

- Goods received were not as described, such as poor quality or wrong color;
- Merchandise was not delivered at all or was damaged;
- A merchant is unwilling to accept returned goods; and
- A cardholder cancels a recurring transaction but the merchant continues to charge the cardholder.

Under the Guide, a cardholder is sometimes required to attempt to resolve the dispute with the merchant before he is able to take advantage of the chargeback rules. There are also different timing requirements for the various scenarios. For example, when the goods were not as described, a claim must be made within 120 days from either the transaction date or the date the goods were received. When dealing with a potential chargeback, a credit union may want to work with its card network representative to ensure the particular scenario involved is covered and the applicable timeframe for filing a claim.

The ever-present threat of fraud only makes these regulations and rules more important to understand and implement correctly. While prompt and thorough investigations of unauthorized use can help mitigate losses, educating members to review their online banking records or periodic statements regularly can be a useful tool in protecting the

credit union. The sooner the credit union knows there is a problem, the quicker it can take steps to ensure no more unauthorized transactions are conducted. This is essential in mitigating losses since both the federal regulations and the card network rules place strict limitations on how much money credit unions may recover from their members. As there is no sign that fraudulent transactions are going away, the risk of loss remains a key issue for credit unions.

FRAUD LOSSES: MITIGATING THE RISKS

Fraudulent transactions pose great risk to credit unions – not only in the direct losses they cause but also in the costs to detect fraud and prevent future harm. When a member's debit card is stolen, a credit union incurs costs to investigate the fraud, monitor the account and issue a new debit card. Not to mention the time it costs the credit union to conduct these activities. If the credit union or the member is unable to find the fraudster and recover the funds, the credit union can be on the hook for the member's losses as well. As a result, credit unions have a vested interest in detecting fraud early and mitigating the risks that it will happen at all.

In 2017, the Fraud Mitigation Survey was conducted by the Payments, Standards and Outreach Group at the Minneapolis Federal Reserve Bank to gauge what financial institutions are doing to mitigate fraud risks. The survey looked at the fraud rates, the efforts institutions employ to combat fraud, the effectiveness of these efforts and the challenges institutions face. The survey respondents included banks and credit unions from across the country, representing both large and small asset sizes.

Overall, three-fourths of all respondents reported fraud losses in 2016. Larger institutions experience higher rates of fraud losses than smaller institutions – 100% of institutions over $1 billion in assets reported fraud losses while only 46% of institution under $50 million reported fraud losses. Debit cards appear to be the most susceptible of the various payment types surveyed – 96% of the respondents experienced debit card losses. Credit card and check losses followed closely with 77% and 74%, respectively. ACH, wire and prepaid losses were experienced much less frequently – 24%, 13% and 7% respectively.

When looking at how financial institutions mitigate these losses, the survey looked at four key areas: account opening, authentication, transaction screening and reporting and risk management. At account opening for new deposit accounts, the most widely used and

most effective methods for fraud mitigation were the Customer Identification Program and requiring new customers to submit account applications in person; 58% of respondents impose an in-person requirement for new customers. For new credit cards, pulling a credit report and using an identity verification service were the most effective methods for mitigating fraud losses.

When it comes to authentication, institutions employ a product specific approach. For cards, PIN authentication, chip authentication and card security code verification ranked as the top three most used and most effective methods to mitigate card fraud losses. Other methods included verifying the cardholder's address and magnetic stripe authentication. For checks, the top methods were requiring access credentials for remote deposit capture services and verifying the signature. Requiring an ID and password was the most used and most effective authentication method for mitigating ACH fraud losses; followed closely by multi-factor authentication. Forty-one percent of institutions reported that they verify the IP address of the consumer for ACH transactions, though only 19% reported this as a very effective method for mitigating losses. For wires, 70% of institutions reported that telephone callback verification was the most effective authentication method.

Transaction screening can be a useful tool in mitigating fraud losses as it allows institutions to detect potentially fraudulent transactions. For both debit and credit cards, blocking or scoring transactions from high-risk countries was ranked as the most used and most effective screening method. This was closely followed by out-of-pattern activity and behavior analytics. For checks, ACH and wires, manual review was ranked in the top two most used and effective screening methods. Reviewing large dollar items was the most effective method for mitigating check losses. For remote deposit capture, limiting the total deposit value, per item deposit value and the number of items deposited were the most used screening methods. OFAC monitoring was the most effective screening method for mitigating ACH losses and the second most effective method for mitigating wire losses.

Institutions rely on a variety of general risk management strategies and internal controls to mitigate fraud losses. Some of the general risk management strategies include reissuing cards that have been breached, providing customers with online access to transactions and statements, applying exception holds to checks, limiting ACH and wires to domestic transfers, refusing to process wires when fraud is suspected, alerting customers to potentially fraudulent transactions and educating staff and customers to

detect and prevent fraud. Some of the internal controls that institutions employ include segregating duties within payment processes, imposing electronic and physical authentication requirements to access payment processing functions, prohibiting the use of personal devices to process payment transactions and timely addressing issues such as chargebacks and returns.

As smaller institutions, it can be more difficult for credit unions to absorb fraud losses. It can be just as difficult to employ sophisticated monitoring programs because of the cost barrier. As the push toward electronic payments continues to spread, mitigating the risk of fraud losses will also continue to be an essential part of a credit union's operations. The methods discussed in the survey provide a menu of options for credit unions to choose from. Though the best method will depend on the credit union's risk profile and particular scope of operations, a combination of various methods can sometimes be the best choice.

ELECTRONIC CHECK COLLECTION AND RETURN

In addition to the compelling statistics on fraud, the Payments Study also revealed another interesting trend: despite the consistent decline in the use of checks, they remain the second largest type of noncash payment by value. In 2015, 17.3 billion checks were paid for a total value of $26.8 trillion. Checks continue to be a top payment method for businesses and many consumers still use checks for certain regular large dollar payments, such as rent and mortgage payments. However, the way checks are being written and processed has been changing in recent years.

Beginning in the early 2000s, information from checks began being processed electronically rather than a physical check being mailed across the country. After the passage of the Check 21 Act in 2004, electronic processing spread rapidly. Today, nearly all checks are processed electronically. As a step further, some payment processors no longer need a physical check at all; they can generate a check solely from information. In an effort to align the regulations with these trends and encourage the use of electronic checks, the Federal Reserve issued a final rule in 2017 amending Regulation CC. One notable change to the regulation is that it will now apply to electronic checks. The rules discussed below become effective on July 1, 2018. As Regulation CC applies to all checks, the rules below apply to both consumer and business checks.

Electronic checks have been used for many years, so internally credit unions may have a

general understanding of what an electronic check is. However, industry lingo does not always align with regulatory definitions so it is helpful to start with a few key definitions. The final rule adds three definitions to section 229.2: electronic check, electronic returned check and electronically-created item. All electronic checks and electronic returned checks start out as paper checks. In order to be considered an electronic check, credit unions must send both an electronic image of the paper check and electronic information to the receiving bank. If a credit union does not send both items, the check is not considered an electronic check under the rule.

If there is no initial paper check but both an electronic image and electronic information are sent, then the payment is an electronically-created item. Electronically-created items are sometimes referred to as "electronic payment orders" and can resemble electronic images of paper checks or remotely created checks. Electronically-created items cannot be used to create substitute checks that are equivalent to an original paper check. Online bill payment systems that collect account information are among the most common users of electronically-created items.

Returned Checks

All of Regulation CC's Subpart C regarding the collection of checks will apply to electronic checks and electronic returned checks as if they were paper checks, including the returned check provisions. In order for credit unions to send and return checks electronically, there must be an agreement in place between the credit union and the receiving bank, or between the credit union and the clearinghouse.

The final rule changes the timeframe and notice requirements relating to returned checks. If a paying bank decides not pay a check, the rule now requires it to return the check so that it would normally be received by the depositary bank no later than 2 p.m. on the second business day after the check was presented to the paying bank. Previously, the rule required return by 4 p.m. Both the time zone and business days are determined by the depositary bank. For example, if the second business day is not a banking day for the depositary bank, the paying bank has until 2 p.m. on the depositary bank's next banking day to return the check. The rule does not require the depositary bank to actually receive the returned check by the 2 p.m. deadline; paying banks may rely on the depositary bank's availability schedules to determine whether a returned check would normally be received by the depositary bank by the deadline. If a credit union fails to comply with these timing requirements, it can be held liable to the depositary bank for all losses incurred up to the full amount of the check. It may also be

liable under state law.

The Check Return Timeframe in Action

Your credit union is located in New York City. It is open Monday through Saturday from 8:00am to 5:00pm. The depositary bank is located in Los Angeles. It is open Monday through Friday from 10:00am until 6:30pm.	A check from the depositary bank is presented to your credit union on Thursday morning.	Your credit union has until 2pm PST on Monday to return the check because the depositary bank is not open on Saturday. The fact that Saturday is a banking day for your credit union is irrelevant.

The paying bank must also send a nonpayment notice to the depositary bank if it determines not to pay a check of more than $5,000. This notice must be sent so that it would normally be received by the depositary bank no later than 2 p.m. on the second business day after the check was presented. Like the return rule, both the time zone and business days are determined by the depositary bank. Notice may be provided by any reasonable means but must include, to the extent possible, the information from the MICR line, payee's name, amount, indorsement date by the depositary institution, trace or sequence number associated with the indorsement, bank name, routing number and the reason for nonpayment.

If the check is unavailable for return, the rule requires the paying bank to send a notice in lieu of return. The notice must include a copy of the front and back of the returned check. If a copy is not available, the notice must include the same items outlined above for a nonpayment notice. The notice must also state that it is a notice in lieu of return. If a depositary bank receives a returned check, nonpayment notice or notice in lieu of return, the rule requires the bank to inform its customer.

Warranties and Indemnities

The final rule also added a number of provisions to section 229.34 on warranties and indemnities to address the changes to the scope of Regulation CC. The rule added specific warranties for electronic checks and electronic returned checks and indemnities for electronically created items. The warranties for electronic checks apply in addition to the other warranties contained in section 229.34 and, unless otherwise stated, these other warranties apply to both paper and electronic checks.

Revised paragraph (a) provides the warranties for electronic checks and electronic returned checks. Under the rule, any credit union that transfers or presents an electronic check or electronic returned check and receives settlement or other consideration for it

warrants that: (1) the electronic image is an accurate representation of the information on the paper check; (2) the electronic information accurately reflects all information on the MICR line and the amount of the check; and (3) no person will have to pay a check that has already been paid, such as in the case of double presentment.

Any credit union that transfers or presents an electronically-created item and receives settlement or other consideration for it must provide indemnification against losses to any transferee bank, paying bank and any subsequent collecting or returning bank. The indemnification must cover losses resulting from the fact that the electronic image and information do not come from a paper check, the member did not authorize the amount or payee stated on the item or payment of an item that has already been paid. The amount of indemnification is limited to the amount of the loss plus interest and expenses.

Remote Deposit Capture

One issue that credit unions often battle is that technology moves much faster than the regulations. While electronic collection and return started before the Check 21 Act, it was not until after its passing that electronic processing became the standard. Without a clear framework or rules governing the playing field, institutions had to rely on each other to set the rules. In this type of environment, rules can vary widely from place to place, making it hard to do business consistently across the country. Recently, we have seen similar issues with the rules governing remote deposit capture. While things like standard contracts and clearinghouse rules have made it easier for credit unions to function in the absence of a clear regulatory framework, it would nonetheless be helpful to have some uniform rules.

While some had hoped that an amended Regulation CC would provide clarity for remotely deposited items, these items remain largely governed by contract. The amendments do not change any of the funds availability rules. As it is not clear whether these types of deposits fit into the availability rule's definition of a check, credit unions will still need to look to state law, such as the Uniform Commercial Code, and their contracts, those it has with its members and with its clearinghouse, to determine the availability requirements for remotely deposited checks. The amendments also do not really provide a stance on the collection and return requirements for these deposits. The preamble does explain that when information from a remotely deposited check is used to create an electronic check or a substitute check, then the appropriate rules will apply. However, depending on the particular software, this may not always be how these deposits are processed. Credit unions may need to consult with their remote deposit

vendors to determine how the collection and return rules apply to these deposits.

The final rule does provide one clear position on remote deposit capture – indemnity. New section 229.24(f) covers the scenario where a check is deposited via remote deposit capture at one institution and that same check is later presented for deposit at another institution. The rule requires a depositary bank to provide indemnity if: (1) it is a truncating bank because it accepts a deposit of an electronic image of a check, (2) it does not receive the original check, (3) it receives settlement for an electronic check related to the original check, and (4) the check is not returned unpaid. If these conditions are met, the bank who accepts the original paper check is indemnified against losses incurred because the check had already been paid.

The Federal Reserve Board believes that this indemnity provision properly allocates losses because the institution that accepts remote deposits is in the best position to minimize such losses. This may include efforts to educate members about remote deposit services. For example, informing members that a restrictive indorsement, such as "for mobile deposit only," is required on all remotely deposited checks. If a credit union employs this strategy, outreach to the remote deposit vendor may also be necessary to determine whether the software is sophisticated enough to reject an image that does not bear the restrictive indorsement.

Restrictive indorsements can be an important safeguard as the rule provides an exception to the indemnity provisions for checks containing a restrictive indorsement. When a bank accepts an original check bearing an indorsement that is inconsistent with the deposit method, it is not entitled to indemnity. For example, if a teller at a branch accepts an original check with a "for mobile deposit only" indorsement, that bank may not seek indemnity for losses when the check is returned.

In finalizing these rules, the Federal Reserve Board recognized that much of the framework for electronic checks is already in place by agreement – whether between individual institutions or through clearinghouse rules. By incorporating these rules into the regulatory framework, the Board hopes to further encourage the use of electronic payments as they are safer and faster than their paper equivalent.

FASTER PAYMENTS: SAME DAY ACH

Beginning in 2016, NACHA began implementing its Same Day ACH initiative. The initiative seeks to expedite the process for sending and receiving ACH payments and is a direct response to industry's call for faster payments. Upon completion of Phase 3, nearly all ACH credits and debits will be processed the same day – only international transactions and transactions over $25,000 will not be covered. The Same Day ACH rules were implemented in three phases.

Phase 1	Phase 2	Phase 3
• Effective September 23, 2016 • Covers ACH credits • Imposes two submission deadlines for processing ACH credits: 10:30am EST and 2:45pm EST • Imposes two settlement times for ACH credits: 1:00pm EST and 5:00pm EST • Requires ACH credits to be available by the end of the RDFI's processing day	• Effective September 15, 2017 • Covers ACH debits • Imposes two submission deadlines for processing ACH debits: 10:30am EST and 2:45pm EST • Imposes two settlement times for ACH debits: 1:00pm EST and 5:00pm EST	• Effective March 16, 2018 • Requires ACH credits to be available by 5:00pm of the RDFI's local time

NACHA expects the Same Day ACH rules to provide a number of benefits to industry. From the consumer perspective, same day settlement allows consumers access to funds sooner and also allows them to pay bills and make other payments the same day. Payroll funds may be used the same day and person-to-person transfers can be delivered quicker. This can be especially convenient for low-income consumers or those with an unpredictable cash flow. From the business perspective, same day settlement allows businesses faster access to payments and other funds coming in. Invoices can be paid the same day and claims or refunds can be accessed quicker, such as from an insurance payout or disaster recovery assistance. This can be especially important for smaller businesses.

As part of the Same Day ACH implementation process, NACHA has been collecting various data to assess the process. In 2017, 75.1 million Same Day ACH transactions were made with a value of over $87 billion. Ninety-two percent of all Same Day ACH debits were consumer bill-pay transactions and account-to-account transfers. The remaining 8% represents business-to-business payments. Same Day ACH credits were more diverse –

47% for payroll direct deposit, 33% for business-to-business payments, 12% for person-to-person transfers and 8% for consumer bill-pay transactions. The value of the various types of ACH debits and credits largely mirror these breakdowns.

NACHA's data has also revealed no increase in fraudulent ACH transactions since September 2016. Unlike the overall transition from cash to electronic payments, the move toward Same Day ACH does not create any new avenues for fraud. NACHA actually expects Same Day ACH to mitigate some of the factors that give rise to fraudulent ACH transactions and other payments risk factors. For example, institutions will carry less credit and settlement risk. Funds are moving through settlement accounts twice per day, therefore cutting down on the length of time these funds are held and mitigating the risk that those funds will not end up reaching their final destination. While debits are not currently required to be available the same day, the Same Day ACH rules do move up the timeline for processing debits by one day. This allows institutions to discover any settlement issues sooner. For example, an originating institution will find out a day earlier that an account does not have sufficient funds to cover the debit. This, in turn, reduces non-sufficient funds risk.

As Same Day ACH moves past Phase 3, NACHA hopes its success will lead to an expansion of the Same Day rules. This may include adding more submission and settlement times, requiring same day availability for ACH debits, increasing the dollar limit on covered transactions or processing transactions on weekends or holidays. In the coming years, both industry and consumers should only expect further progress in this area.

CONCLUSION

Electronic payments are here to stay. In the coming years, the use of electronic payments will only continue to increase and faster payment technologies are already showing up on the market. Products such as mobile wallets offer consumers quicker and more convenient ways to pay for goods and services and many companies have developed apps that allow consumers to save payment data. As the regulations are not nearly as sophisticated as these technologies, more questions and risks will continue to arise. For example, would a credit union need to follow the error resolution procedures when an app gets hacked and fraudulent transactions are made but no payment information is obtained?

As industry continues to adapt to this transition, credit unions may need to ensure they are prepared to face the challenges and emerging risks. It is important to ensure regulatory and contractual obligations are met to protect against losses from unauthorized use and other fraudulent transactions. As the regulations struggle to keep pace with technology, contractual obligations will continue to be as important to know and understand as any regulatory obligations. Credit unions may also need to ensure they have the infrastructure in place to keep up with these technological advances and the rapid pace of payments processing.