

INSIDE: Important Information Regarding 2019 ACH Rules.....	pg. 1	"Oops" is a Four-Letter Word with Money-Transfer Apps.....	pg. 5
Restrictive Endorsement Woes.....	pg. 1	Business Email Scam Losses Now Top \$12 Billion.....	pg. 6
European Data Protection Impacting US Based Organizations.....	pg. 1	Visa, Mastercard Reach \$6.2 Billion Settlement Over Card-Swipe Fees.....	pg. 6
Retaining and Reproducing ACH Authorizations: What Are My Time Frames?.....	pg. 2	SMB Employees Fail to Take Cyber Threats Seriously.....	pg. 8
Understanding OFAC: A Best Practices Compliance Guide for All Businesses.....	pg. 3	Kroger to Expand Visa Credit Card Ban to More Stores.....	pg. 8
Visa: Chip Cards Reduce Counterfeit Fraud at US Merchants by 75%.....	pg. 5		

Important Information Regarding 2019 ACH Rules

NACHA has discontinued the *ACH Rules – Corporate Edition*. This will ensure all ACH system participants are accessing the full and complete version of the *ACH Rules*. The online and app version of the *Rules* have

been also enhanced with additional search functionality to allow users to quickly find the *Rules* references they need.

To order the 2019 *ACH Rules*, please contact your financial institution. 📞

Restrictive Endorsement Woes

by Marcy Cauthon, AAP, APRB, NCP, Director, On-Demand Education

On July 1, 2018, Regulation CC amendments became effective for financial institutions. With these new amendments came changes around Remote Deposit Capture (RDC) checks. There is now a new RDC Indemnity in place that says if a check is processed via any form of Deposit Capture and the paper check related to the image is processed again, the institution who holds the paper check may try to recover funds from the institution that took the check via Deposit Capture. This is a significant change for financial institutions but what does it mean for account holders? The regulation states

that if the paper check has any kind of a restrictive endorsement on it, then this RDC Indemnity cannot be filed.

That said, your institution may have recently put restrictions on how checks deposited through a capture service are endorsed. Below are some different variations of what you as an account holder may



see WOES on page 4

European Data Protection Impacting US Based Organizations

by Karen Sylvester, AAP, CAMS, CRCM, NCP, Director, Compliance Education

There is a new abbreviation abroad that may be impacting those of us in the United States. The General Data Protection Regulation (GDPR) was designed by the European Union (EU) member nations to create a uniform standard of consumer data privacy protection for all companies that do business in the EU. The regulation concerns itself with the privacy of EU citizen data and has some similar goals to our own data protections in the United States, but also has additional requirements.

GDPR applies to entities physically located within the EU member countries, but the regulation could, under certain circumstances, reach “across the pond.” In theory this COULD include your organization. It really boils down to this: do

see EUROPEAN on page 2

EUROPEAN continued from page 1

you have any EU citizens, or dual US/EU citizens, on your list of clients? If the answer is “no,” then, in all likelihood, you can rest easy unless you are actively marketing to EU citizens.

All entities holding information about EU citizens are required to abide by the newest regulation. Below are a few key areas where GDPR takes things a step further:

1. **Right to Be Forgotten/Right to Erasure** – EU citizens covered by GDPR have a right to request that any and all personal data you have on them be corrected (if inaccurate) or deleted entirely. A key note here is that this is only required if the individual makes such a request. And, even then, the organization would have 30 days to respond.

2. **72-Hour Breach Notification** – If your organization experiences a breach, you’ll have 72 hours from that point to notify the supervisory authority in the member state in which your customer/member resides. Entities should provide a notice to its customers whenever it becomes aware of an incident of unauthorized access to customer information and, at the conclusion of a reasonable investigation, if it determines that misuse of the information has occurred or it is reasonably possible that misuse will occur.

3. **Explicit Opt In Requirements** – Essentially, EU citizens must both opt in to what information will be collected about them and must agree to every way in which that data is used prior to those actions taking place.

4. **Contracts** – Entities with Third-Parties transmitting, processing or storing EU citizen data should spell out how the exchange and use of data will work with data processors, and for what each party is responsible. In practice, this would just become a deeper dive during due diligence/on-going monitoring of your Technology Service Providers.

What does this mean for a business? Know who your customers are and where your customers are from. Know what information you hold and know if a breach happens you must notify the impacted customers promptly.

EPCOR will continue to monitor for guidance or regulatory changes from the US regulators. 🌱

Retaining and Reproducing ACH Authorizations: What Are My Time Frames?

by *Jennifer Kline, AAP, APRP, NCP, Director, Audit Services*

As an ACH Originator or company initiating ACH transactions, it is a business’s responsibly to obtain a proper authorization from the Receiver of the transaction.

Once you’ve sent the prenotification, set up the recurring payment and everything is working fine, what do you do with the Receiver’s authorization? Place it in a file, a cabinet, maybe File 13 or “the circular file?” What should your proper procedures be to satisfy

the rules and regulations that apply to that transaction? What will happen if your financial institution requests a copy of an authorization? Will you know where it is? Or, will it feel as if you’re sending someone on a snipe hunt?

To remind you of what you most likely agreed to with your financial institution,

and what is stated in the *ACH Rules*, you should be obtaining a clear and readily identifiable authorization, including verbiage for the Receiver with the right to revoke the authorization in a specific time and manner. The authorization can be obtained by either a paper/written method or a similarly authenticated method compliant with the E-Sign Act¹. Likely, when you began ACH services with your financial institution, you were provided with samples of proper language for both credit

see **AUTHORIZATIONS** on page 4



¹ The Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq).

Understanding OFAC: A Best Practices Compliance Guide for All Businesses

Over the last decade, the Office of Foreign Assets Control (OFAC) has imposed \$4.3 billion in civil money penalties. But, did you know that businesses other than financial institutions received 81% of these fines last year?

Yes, OFAC violations are costing US businesses hard-earned cash. Since the attacks of September 11, 2001, OFAC's role in national security has increased immensely. The passage of the US Patriot Act brought with it a broader definition of the term "financial institution" in order to highlight industries that, by their very nature, are at a heightened risk for money laundering and OFAC violations. Those industries are defined by OFAC as "All Other Businesses."

OFAC Fines are Costing "All Other Businesses"

From 2006 to 2017, nearly 30% of all fines levied against OFAC's "All Other Businesses" category ranged from \$100,000 to \$499,999. For many companies, a penalty that hefty could be enough to put them out of business. Even if not, an OFAC violation could cause irreparable reputational harm that affects profitability for years to come. Here are just a few of the maximum penalties OFAC can levy against businesses:

- Up to \$20 million in criminal penalties and 30 years in prison for willful violations of some programs
- Up to \$1.4 million in civil penalties for each violation of the Foreign Narcotics Kingpin Designation Act

- Up to \$85,236 for each violation of the Trading with the Enemy Act

With the stakes so high, companies across all types of industries must understand the importance of OFAC compliance and take proactive steps to avoid a compliance pitfall.



Protect Your Business with Sanctions Screening

The crux of your OFAC compliance program is its denied party screening process. Sanctions lists are updated every time OFAC identifies a new individual or entity to be added or removed from that list, which can occur daily. OFAC's various regulations determine your company's risk profile and how often you'll need to cross-check that list: with every transaction, with every new customer, or your entire customer database at periodic intervals.

Understanding OFAC and Sanctions Screening

Comprehending OFAC's role in your industry is the key to a successful sanctions screening program. Download Computer Services, Inc.'s white paper, *Understanding OFAC: A Best Practices Compliance Guide for All Businesses*, to learn how you can enhance your compliance program and mitigate potential risks. In the paper, CSI's regulatory experts offer the intel you need to improve your sanctions screening program, including:

- Detailed analyses and data trends of OFAC fines by type and industry from 2006 to 2017
- OFAC implications for several industries, including insurance, money services businesses (MSBs), nonprofits and others
- Five critical best practices for enhancing your company's sanctions screening program
- Steps to handle positive screening matches

CSI's white paper provides insight on overcoming your toughest compliance challenges and enhancing your sanctions screening program. OFAC compliance is complicated, but the cost of non-compliance is far too steep to risk.

To download the white paper go to <http://bit.ly/ofacwhitepaper>. 📄

Source: *Digital Transactions*

· 2019 ·
NACHA
Operating Rules & Guidelines

The Guide to the Rules Governing the ACH Network

Start 2019 Out Right, With a Fresh Set of Rules!

Ask your financial institution about pre-ordering your 2019 ACH Rules to receive them hot-off-the-press this January. Corporate Users now have full access to the complete ACH Rules!

AUTHORIZATIONS continued from page 2 authorizations and debit authorizations.

Very rarely, possibly 0.01% of the time, would you ever be asked to provide a copy of a credit authorization. In fact, the *Rules* state that credit authorization is not required to be in writing; however, new employees signing up Direct Deposit will gladly complete that authorization along with the new employee documents.


Debit authorizations, on the other hand, are more of a concern. At any time, your financial institution could request to see a copy of a debit authorization. This could be to test procedures and your readiness for audit testing, or because the Receiver's financial institution is formally requesting a copy of the authorization to clear up some type of dispute. Your financial institution has 10

banking days to comply with this request. Consequently, you as the Originator, may have less time to find that authorization.

In your frantic search for that requested authorization, did you need to go through some security controls to find it? Good. You are responsible for ensuring the data on the authorization is protected and secure. The authorization should only be available to those who would need access and not to the general public, so it could be in a locked room or filing cabinet. Or, if authorizations are scanned into a document archival database, then authorizations should have controls as to who can have access.

As you continue in your search, imagine all authorizations are thrown into one big box with no order to it at all. Eek! If you decide to order this chaos, remember authorizations

need to be retained for two years after the termination of the authorization. So, according to the *Rules*, you cannot discard an authorization just because it was signed 20 years ago as it may still be current and in effect. Before any authorization is destroyed, ensure that the revocation for that Receiver is over 2 years.

When replying to your financial institution's request, ensure they have up-to-date information for the department or main person of contact with proper phone and email address. If you have more questions about Receiver authorizations, ask your financial institution or refer to Subsection 2.3.2 Authorization and Notices with Respect to Consumer Accounts of the *NACHA Operating Rules & Guidelines (ACH Rules)*. 

WOES continued from page 1


be experiencing.

Each financial institution makes a business decision on how they are going to handle endorsements on checks deposited via Deposit Capture. That means not every institution is doing the same thing. The level of risk that Deposit Capture brings a financial institution drives what type of endorsement they will require and what entities it will apply. For instance, the RDC Indemnity is based on a duplicate check situation, meaning you have a check clear through a Remote Deposit Capture product and then again as the physical paper check. An institution must weigh the risk of receiving duplicate items. For example, they may receive several

duplicate items a day on account holders that deposit checks via their mobile device while receive few duplicates on checks deposited through remote deposit capture utilized by merchants or businesses. In this case, this institution may decide to leave Merchant Capture client checks endorsed the way they have been receiving them before July 1st. However, since there is a higher risk with Mobile Capture, the institution may request these account holders endorse each paper check as "For Mobile Deposit Only—Financial Institution Name" before taking a picture with their mobile device.

Some institutions have also found that "For Mobile Deposit Only" may be too restrictive in some cases, so they have decided to have

their Mobile Capture users endorse the paper check as "For Deposit Only—Financial Institution Name." This helps when a user has trouble depositing through Mobile Capture and must take the item inside the financial institution, a drive-up window or ATM. By putting this more generic restrictive endorsement on the check, it allows the check to be deposited only at that certain institution, but through several channels.

Again, you may have noticed some changes in endorsements with capture products in the last few months. Hopefully you now understand why your institution made those changes and why products at different institutions may require different types of restrictive endorsements. 



Real-Time Interbank Settlement
Same Day ACH Rule Changes
ISO 20022 Adoption
Regulation CC Changes
EMV Deadlines
Regulatory Updates
Fraud Considerations

There Are HUGE Changes Coming in the Payments Industry!

Find out what you need to know to prepare for 2019 and beyond at EPCOR's one-day *Payments Systems Update* seminar.

Visit epcor.org for a list of locations and to register.

Visa: Chip Cards Reduce Counterfeit Fraud at US Merchants by 75%

Data released by Visa showed that counterfeit fraud ticked down at US merchants by 75% from September 2015 to March 2018 as more storefronts started accepting chip cards.

To that end, Visa said that, as of its latest “Visa Chip Card Update,” as many as 67% of storefronts in the United States now accept chip cards.

The company further elaborated that counterfeit fraud dollars at *all* US merchants slipped 46%.

Looking at the Visa chip card count out in the field, June’s number stood at 499.7 million. That’s up from 159 million in September 2015. The 214% increase comes

as 69% of cards, including debit and credit, have chips. Breaking down those segments a bit, the company noted that of total chip cards, credit cards were at more than 210 million—up from 93 million in 2015. The total number of debit cards leaped from 67 million to 289.1 million.

The number of merchant locations accepting the cards is at 3.1 million—up from 392,000 locations at September 2015, and up 680% from the beginning of EMV migration in the United States. With the increased presence at storefronts, it makes sense that payments volume would also be on the rise. Visa said that 97% of US payments in June were on EMV cards.

In terms of chip payment volume, the latest reading stood at \$76.7 billion — up from \$4.8 billion in September 2015. The transaction count saw a boost from 79 million to 1.7 billion over that same timeframe.

A previous Visa infographic showed that US financial institutions had issued 462 million chip cards to consumers, and chip cards were accepted at 2.5 million (55%) US storefronts in June 2017. According to Visa, as of September, there were \$59.4 billion in chip transactions, up from the previously mentioned \$4.8 billion in September 2015.

Source: Pymnts.com

“Oops” is a Four-Letter Word with Money-Transfer Apps

Anthony MacDonald was perplexed when \$16 and a hamburger emoji showed up in his Venmo account from Zach Brown. The name didn’t ring a bell.

More money followed: a \$35 payment, then \$19. Another \$15 arrived with a mysterious message: “Meatball shop without gada.”

That’s when the 27-year-old, who works in youth ministry at a church in Delaware, decided he should stop taking Mr. Brown’s lunch money.

With the rise of money-transfer apps such as PayPal Holdings Inc.’s Venmo, it’s never been easier for people to send money to their friends. It’s also never been easier to accidentally send money to a total stranger.

Getting the money back is often far more difficult: many digital payments are irreversible.

For the recipient, it’s the equivalent of finding cash on the sidewalk—except it comes with a moral quandary.

At first, Mr. Brown’s errant Venmos

amused Mr. MacDonald. “Keep it coming,” he jokingly tweeted.



But after talking it over with colleagues at his church, he decided the charitable thing to do was fess up.

He returned the last \$15 payment but not the other \$70, which he’d already transferred to his bank account.

“Sorry man,” he wrote on Venmo to Mr. Brown, whose apparent mistake was turning McDonald into MacDonald. Mr. Brown didn’t respond to requests for comment.

Venmo links to bank accounts or credit cards of users identified by unique handles, letting them send payment to other Venmo users with just a few taps on their phones. The app allows users to include a message with their payments; emojis are popular.

Users can search or scroll through lists of others who are on the service, but typing one wrong letter can pull up the wrong person with a similar handle or name.

New money transfer services have popped up; a consortium of financial institutions launched their own money transfer app, Zelle, last year. Facebook allows people to transfer cash through its Messenger app.

But Venmo, founded in 2009, popularized money transfer apps as a way to quickly repay friends. Much like Uber, the ride-sharing service, Venmo became ubiquitous and morphed into a verb.

Venmo, which moved around \$12 billion in payments in the first quarter, according to the

[see OOPS on page 7](#)

Business Email Scam Losses Now Top \$12 Billion

The US Federal Bureau of Investigation released a public service announcement warning that business email compromise (BEC) scams are on the rise.

The total value of funds redirected due to a BEC scam has now topped \$12 billion, the

FBI said, updating previous warnings of the scam and including data up to May 2018. Between December 2016 and last May

there was a 136% increase in BEC scam losses across the globe, the FBI said, and instances of the crime have been reported in 150 countries and all 50 US states.

Analysis shows banks in China and Hong

Kong are the top destination for redirected funds, stolen when a scammer emails a business by infiltrating a legitimate email account, and requests a transfer of funds or other sensitive data. The emails often appear as legitimate requests such as, for example,

a request for invoice payment from a supplier.

According to the FBI, the Internet Crime Complaint Center (IC3) recorded 41,048 US

victims of BEC scams between October 2013 and May 2018, totaling more than \$2.9 billion in losses.

The FBI warned that the real estate sector is an increasingly popular target for business

email compromise scammers, including total companies, law firms, real estate agents and property buyers and sellers, the announcement said. Between 2015 and 2017, the real estate market saw a more than 1,100% increase in the number of BEC victims.

An announcement by the FBI issued in 2016 pinpointed Hong Kong as ground zero for many business email scams identified. At the time, total losses and attempted losses reached \$3.1 billion. At the time, the FBI reported a 1,300% increase in the value of losses between January 2015 and June 2016, while reports of BEC scams had increased by 270% in the first half of 2016.

EPCOR has put together a five-minute *Did You Know* video which helps explain BEC scams in less than five minutes. To watch, search EPCORPymnts on YouTube and click on the video. Please feel free to share the video with your staff or other businesses to help raise awareness of this dangerous scam.

Source: Pymnts.com



Visa, Mastercard Reach \$6.2 Billion Settlement Over Card-Swipe Fees

Visa Inc, Mastercard Inc, and a number of US banks agreed to pay \$6.2 billion to settle a long-running lawsuit brought by merchants over the fees they pay when they accept card payments.

Visa and Mastercard previously reached a \$7.25 billion settlement with the merchants in the case, but that deal was thrown out by a federal appeals court in 2016 and the US Supreme Court last year refused to revive it.

The deal had been the largest all-cash US antitrust settlement, although its value shrank to \$5.7 billion after roughly 8,000 retailers opted out.

The card issuers named in the class-action

lawsuit include JPMorgan Chase & Co, Citigroup and Bank of America.

The lawsuit, brought on behalf of about 12 million retailers and dating back more than a decade, accuses the credit card companies of violating federal antitrust laws by forcing merchants to pay swipe fees and prohibiting them from directing consumers toward other methods of payment.

In rejecting the earlier settlement, which was opposed by retailers including Amazon.com Inc, Costco Wholesale Corp and Walmart Inc, a federal appeals court found that the accord was unfair because some retailers would receive little or no benefit.

The card companies have already paid \$5.3 billion and will now pay an additional \$900 million.

Mastercard will pay an additional \$108 million from funds set aside in the second quarter, the company said.

Visa's share represents around \$4.1 billion, which the company expects to pay using funds previously deposited with the court, and from a litigation escrow it set up on June 28.

The settlement must still be approved by a court.

Source: Reuters.com

OOPS continued from page 5

company, doesn't publicly report how often money is sent to the wrong person. In an age of instant money transfers via mobile apps, it's no longer an uncommon phenomenon. People can make the same mistake on other, similar apps.

In the six years since its public launch, Venmo has incorporated several fail-safe measures to prevent mistaken payments, according to a Venmo spokeswoman. An algorithm now flags payments to new recipients. Venmo also added profile pictures, which can help identify the right person. There's also the option of using codes that are unique to each user.

Accidental payments still make it through the system. Venmo advises users who mess up to send a message through the app requesting the money's return. It works—sometimes.

Emily Dunn, a student at San Jose State University in California sent about \$45 to a friend named Riley along with a humorous message. He was confused when she later asked if he thought her message was funny. She had mixed up his last name, sending the money to the wrong Riley.

Panicked, Ms. Dunn sent Riley-the-stranger a payment request. After several days brought no response, she figured it was hopeless. Finally, on day four, Ms. Dunn got a transfer notification. Stranger Riley had returned the money. "GOOD PEOPLE DO EXIST!" Ms. Dunn gushed on Twitter.

Nick Abouzeid, a 21-year-old in San Francisco who works at a tech startup, received an unexpected \$149 from a stranger along with the message "for a wonderful evening." Two minutes later, he got another message: "I again made a mistake :(((

He decided to investigate. (The app allows users to view the transaction history of others, depending on their privacy settings.) The account, he found, was brand new. He ran the user's profile picture through Google's reverse image search engine and saw it used in other places. He also saw the user sent

money to another person "for lesbian game," and a minute later wrote to that person: "wrong person, please refund." Mr. Abouzeid was convinced it was a scam. "At that point I had no sympathy," he said.

The user continued to plead for the money. "I was just wrong! Stop spoiling my life Nicholas." Another message request for \$149: "Swindler, return my money, I was wrong!!"

Mr. Abouzeid shared the messages with Venmo customer support and some friends. Venmo, he said, canceled the \$149 transfer before Mr. Abouzeid moved it to his bank account. The company said it has procedures in place to deal with fraudulent transactions.

One friend sent the user \$2. "Don't let Nicholas bring you down!" he wrote on Venmo. "What a buzzkill." The account is no longer active.

Some Venmo users don't even notice that they've sent money to the wrong person.

Gerald Woods never heard back from a Venmo user he didn't know, who sent him almost \$200 that Mr. Woods deduced was meant for another Gerald Woods.

Mr. Woods, who owns a moving company in Minneapolis, asked his Facebook friends what he should do with the money.

Several of them advised him to enjoy the good fortune, Mr. Woods said. "Mailbox blessing?" one friend wrote. "Depends on the amount," another posted.

Mr. Woods decided to return the money. "If you have any type of spiritual connection, whether you call it karma, or the universe, it comes back to you in some way," he said.

Some friends were unimpressed. One sent him an animated GIF of a dog shaking its head, and another suggested Mr. Woods had fallen for a scam.

All he got from the mistaken sender was a terse thank you.

"It was a little less than I expected," Mr. Woods said. "A tip, maybe?"

Source: Wall Street Journal



Are the Letters NCP in Your Future?

CHECK REGULATIONS ARE CHANGING!

Conquer them by becoming a National Check Professional with help from EPCOR's *NCP Prep Program* that has produced NCP exam top scorers for six years running!

Visit epcor.org for details and to register.



Could You Use Some Expert Payments Advice?

If you are considering accepting a new payments type, need a little help creating payments policies or procedures or have any other payments project in the works, EPCOR Advisory Services can help.

Visit epcor.org to find out more about Advisory Services and request a no-obligation quote!



Are You a Third-Party Sender?

If so, don't forget your **ACH Rules Compliance Audit** must be completed by **December 31st!**

EPCOR's *Third-Party Sender ACH Audit Workbook* will walk you through the process.

Or, if you would like an outside set of eyes, contact LarryM@epcor.org to schedule a professional audit with EPCOR.

SMB Employees Fail to Take Cyber Threats Seriously

Unfortunately for small-to-medium-sized businesses (SMBs), many employees remain ignorant to the reality of cyber threats and make decisions that continue to put the company at risk, according to a study from Switchfast Technologies.

The study found that one in three business owners do not have safeguards in place to combat cyber breaches and 60% of small businesses that suffer a breach go out of business within six months. With legislation like the National Institute of Standards and Technol Small Business Cybersecurity Act being put in place, it's clear that cybersecurity has become a weakness for SMBs.

In large part, employees remain unaware of the cybersecurity threats they face both in and out of the office, in part because the businesses themselves are not taking cybersecurity seriously. The study found that 35% of employees haven't changed their work email password in the last year. Risks to business from weak password policy is compounded by the number of employees (19%) who share their passwords with colleagues. The same number of

employees reported that they use personally identifiable numbers (birthday, anniversary, Social Security numbers) in their work email password.

In addition, 26% do not know what the dark web is, which means that they are also unaware that their personal data may be on it. All the while, few organizations are reportedly providing cybersecurity guidance to their employees. Nearly 21% of those surveyed said their company has never provided cybersecurity training and 65% said their company has never run a phishing email test.

"Today's cybercriminals employ a variety of complex attack methods to exploit business weaknesses and target employees with bad cyber hygiene, whether it's the CEO or an intern, bypassing the basic security measures most companies have in place," according to the report.

"Until they recognize they are prime targets for hackers and adjust their security strategies, small businesses will continue to fall victim to rampant cyberattacks."

Source: *InfoSecurity-Magazine.com*

EXPLORE EPCOR MEMBERSHIP

EPCOR has membership opportunities for companies, businesses, corporations and Third-Parties.

Explore your options, call **800.500.0100** or email memserve@epcor.org.

EXPLORE EPCOR

Kroger to Expand Visa Credit Card Ban to More Stores

Foods Co., part of Kroger's Food 4 Less Stores subsidiary, says 21 supermarkets and five gas stations in central and northern California no longer accept Visa credit cards as of August 14. The decision was made to save on fees. Kroger, the nation's largest grocer, must pay Visa to



process credit card purchases. But the action could be far-reaching.

Kroger is considering expanding the ban to more of its stores if it doesn't reach a deal with Visa on fees at Foods Co. stores.

Source: *Forbes.com*