Payment Compliance:
Same Rules, Different Game

Chris Gonzales
Director of Products and Services,
BillingTree

Ian Winder
Product Manager,
Accounts Receivable Management
Interactive Intelligence, Inc.

Table of Contents

Overview: New Challenges and Opportunities 3
Today's challenge: same game,different rules *3*
Working towards a win-win: technology & processautomation *4*
The Changing Landscape of Payment Compliance 5
Securing Data: PCI DSS 6
Payment fraud is on the rise *6*
Solution #1: tokenization *7*
Solution #2: secure IVR *7*
Solution #3: secure audio and screen recording *7*
And there's more to come… *8*
Partnering with service and technology vendors to ensure PCI compliance *8*
Respecting Authority: Payment Authorization Requirements 8
Authorization basics *9*
ACH: double-checking your payment authorization requirements *9*
ACH authorizations: verbal and/or written consent *10*
Card payments: phone or Web authorization tips *11*
With Convenience Comes Complexity: Convenience Fee Quandaries 12
At the center of an ongoing debate: who pays? *12*
Regulations and guidelines: what is "convenience?" *13*
"Void where prohibited by state or local law" *14*
Risky business *14*
Drawing Conclusions 15
The Authors 17

Interactive Intelligence, Inc.
7601 Interactive Way
Indianapolis, Indiana 46278
Telephone 800.267.1364
www.ININ.com

Publish date: 06/13, version 1

Overview: New Challenges and Opportunities

In an economic climate that can be described as post-recessionary yet in sluggish recovery, the accounts receivable management industry faces unprecedented challenges to their business operations and to their ability to mitigate risks related to the collection and processing of payments. The ascendance of the Consumer Financial Protection Bureau (CFPB) and the increase in regulatory and plaintiff litigation under the Fair Debt Collections Practices Act (FDCPA)[1] has led to a need for a fundamental reexamination of collections business operations and a complete reevaluation of best practices related to collections authorization, validation and reporting. This reevaluation has spilled over and influenced the perspectives and policies of other industry stakeholders, including state and local government regulatory agencies as well as credit card companies.

At the same time, although standards for data security have been well established by the credit card industry through the Payment Card Industry (PCI) Data Security Standard (DSS), the risks of payment card fraud continue to increase[2]. PCI has been described by its critics in the IT field as "a minimum baseline for security," meaning that while compliance to payment card industry standards may help mitigate risk, it does not necessarily prevent fraudulent actors from successfully stealing consumer and merchant information.

In this white paper, we explore some of the unique challenges faced by the ARM industry today specific to collections compliance, and highlight strategies and best practices that can not only mitigate compliance risk, but also improve operational efficiency.

Today's challenge: same game, different rules

Regardless of payment medium, or collections market niche, the name of the game for ARM organizations remains the same: collect outstanding debt as efficiently and cost-effectively as possible while playing by the rules. Sounds simple, right?

Maybe not. The challenges today can be summarized in three ways.

1. **Consumer trends in payment technology outpace regulation.** The option of phone- or Web-based collections, for example, has morphed into mobile, social media- or text-based payment processing. How the old rules apply to new technology always raises new questions and results in ambiguity, introducing a new set of risks and rewards.
2. **Data security standards always lag behind the latest scam.** While ARM organizations focus on meeting existing security requirements, security failures can hurt their reputation, levy significant fines and impact future business. The stakes in the tech battle between security professionals and criminals continue to rise as the rate of online fraud has increased — and there's no end in sight.
3. **Mitigating compliance risk is becoming more problematic.** The classic strategy of avoiding litigation (vs. winning in court) takes on another dimension, because the CFPB can act as a plaintiff and also enforce regulations and impose penalties. ARM organizations may have worked diligently to institutionalize compliant processes; however, they are now reviewing their policies again and

[1]Source: 2013 CFPB Annual Report
[2]Source: 2011 Nilson Report

asking “are they adequate from a CFPB perspective?” At the same time, these organizations are trying to ensure that they are able to present clear and compelling evidence of compliance if and when an audit or lawsuit becomes unavoidable. The new compliance benchmark is not whether a policy is in place, but whether it will serve to prove that the policy is in practice and is working adequately enough to measure up to CFPB scrutiny.

Managed improperly, each of these obstacles can draw enough dollars and resources to bring an organization to its knees. The key, therefore, is to approach compliance in a way that is readily and consistently adhered to — and that is trackable, reportable and flexible enough to change based on new technology trends, security threats and changes to adherence standards. This is where technology and process automation come in.

Almost without exception, companies investing in payment process automation realize immediate benefits and short-term return on investment based solely on efficiency gains.

Working toward a win-win: technology & process automation

Ultimately, the process of evaluating potential compliance risks and identifying opportunities to optimize efficiency go hand-in-hand. Almost without exception, companies investing in payment process automation realize immediate benefits and short-term return on investment based solely on efficiency gains. Then there’s the longer-term benefit of greater confidence and assurance in their ability to demonstrate compliance within an increasingly complex regulatory environment.

Companies that automate payment processing are better able to:

- Avoid credit card company downgrades and chargebacks, while simultaneously reducing the time and effort in processing and reporting.
- Dramatically reduce the cost of dispute handling, as the process of gathering and retrieving payment authorization data and documentation becomes a natural extension of handling a transaction.
- Avoid litigation and defending against lawsuits becomes less costly in terms of time and resources for the same reasons.

The Changing Landscape of Payment Compliance

If an organization collects money on behalf of another company, it is subject to the Fair Debt Collection Practices Act (FDCPA). As of January 2013, the Consumer Financial Protection Bureau (CFPB) now supervises a much broader group of industry players, prohibiting unfair, deceptive and abusive acts and practices and ensuring that collection practices are compliant with federal laws. These laws include, but are not limited to, the FDCPA, the Dodd-Frank Act, the Electronic Signatures in Global and National Commerce Act (E-Sign), and others. New supervisory powers for debt collectors with more than $10 million in annual receipts in debt collection include the ability to review sale contracts, telephone recordings, account transfers, training programs and scripts for employees.

While the authority of the CFPB lies at the federal level, state regulations that are nearly identical to the FDCPA must typically be navigated as well. Regardless of the letter of the law or laws, the interpretations and biases of any governing body have shifted. As a result, the burden of proof and the ability to provide a clear audit trail for any payment process weighs even more heavily on the payee.

Meanwhile, the CFPB has had an impact on consumers, their knowledge and awareness of their rights, with an increase in opportunities to voice their concerns. One example of this is the CFPB establishing the Consumer Complaint Database in March 2013. This has a potential impact on smaller agencies, because even if they are too small to be on the CFPB audit cycle, complaints registered against them in the database may result in CFPB scrutiny.

For decades now, federal and state government agencies have wrangled with credit card agencies over the allocation of payment processing fees. Merchants have joined in the fray to protect their interests, and consumers are revolting at the very threat of passing transactions costs on to them. As Figure 1 illustrates, multiple stakeholders govern the various types of payment transactions.

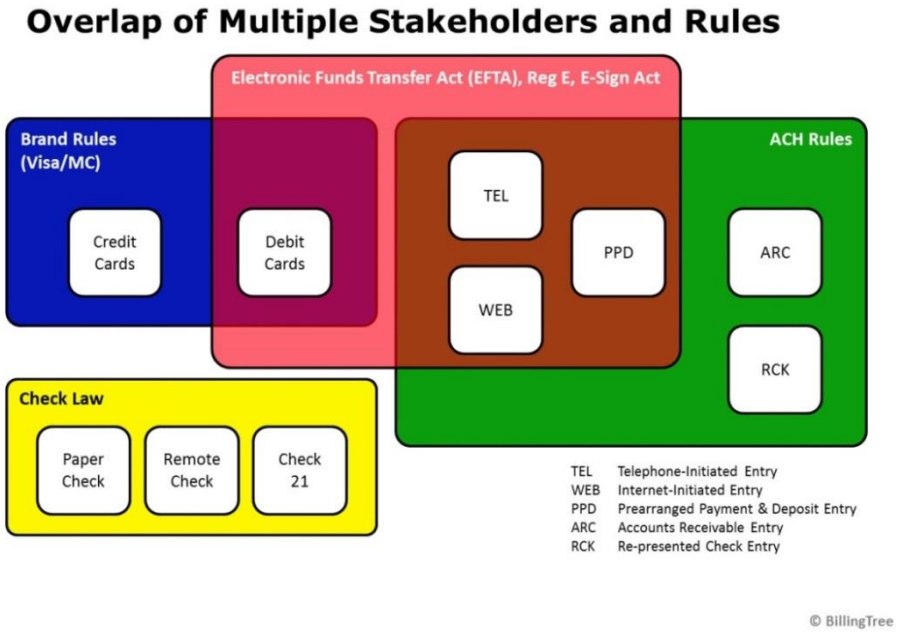


Figure 1: Compliance Stakeholders by Payment Medium

Securing Data: PCI DSS

Before we explore the various payment mechanisms and compliance requirements for authorizations, it makes sense to discuss the requirements and risks associated with the information gathered by payment collectors. This is an area where well-established guidelines have been created, and where interpretations of these guidelines are fairly straightforward. That isn't to say that the guidelines themselves are perfect or complete. For debt collectors, that means understanding how the guidelines contribute to reducing their liability, and at the same time, recognizing the potential exposure to fraud risk and higher costs.

The payment card industry (PCI) data security standard (DSS) was created to increase controls around cardholder data to reduce credit card fraud by limiting its exposure via encryption. Validation of compliance is done annually — by an external Qualified Security Assessor (QSA) that creates a Report on Compliance (ROC) for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes, as defined in the PCI standards.

PCI DSS defines "control objectives" for payment card data, including:

- Maintaining network security
- Protecting card holder data
- Maintaining a "vulnerability management program"
- Implementing strong access control measures
- Monitoring and testing networks
- Maintaining an information security policy

Payment fraud is on the rise

While this framework provides a set of minimum standards to protect merchants and related third parties from data fraud liability, the reality is that payment data theft is on the rise. According to a 2010 Nilson Report, debit card fraud has increased five-fold in the past five years, and debit and credit card fraud losses are expected to reach $10 billion by 2015.

As former U.S. Department of Justice senior counsel Kimberly Peretti described the current environment, federal prosecutors have gone from prosecuting criminals for defacing Web pages a decade ago to targeting international crime rings. High-profile hacks like that of Global Payments in 2012, where cybercriminals stole up to 1.5 million credit card numbers, represent the kinds of fraud risks that merchants and collectors face today.

"We've gone from card farms to card resellers to international hackers," said Peretti.

For third party collectors, complying with PCI DSS compliance will protect them from liability under the terms of their operating agreements with the major credit card companies. This means that the PCI-compliant organization faced with an audit may maintain their ability to process credit or debit transactions, and limit their financial liability when fraud occurs. It does not protect their reputation with their clients or with consumers. Needless to say, those consequences may be dire.

Solution #1: tokenization

One key strategy for preventing the kind of data hacks that lead to stolen debit/credit card data is to ensure that the data is never actually stored or accessed by the payment collector. This approach is referred to as tokenization. PCI-compliant data systems rely on tokenization to ensure that payment data is never exposed to the payment collector.

Simply put, tokenization is the storage of payment card or account information within a secure database outside a merchant's network for use in re-identifying recurring or return customer payments without needing to re-present the card or account information. ***Rather than storing and passing card data, accounts receivable systems merely pass a token to the payment processor's system*** (the same system which assigned the token on the first use).

This process allows customer credit card information to be held, managed and protected by a third party rather than the organization doing the collecting; in essence, removing the risk of a data breach containing personal card information or account data from the collector. It also provides consumers with additional payment flexibility by offering the storage of multiple payment accounts so that they don't have to re-enter account information each time they visit the same merchant or make ongoing payments.

Solution #2: secure IVR

Secure IVR applications are yet another means for helping to ensure PCI compliance by restricting access to cardholder data. When using secure IVR, a consumer can interact with a contact center or collections agent per normal business procedures. However, when the time comes for the consumer to provide their payment information, the consumer is transferred to an automated IVR system where they enter their credit card number into the secure IVR application. During this time, the agent/collector is placed on hold, and is reconnected with the caller once the transaction is completed.

In this scenario, the agent/collector is never exposed to the credit card number or security code.

Solution #3: secure audio and screen recording

There are numerous benefits of call recording within contact centers and collections organizations:

- Establish benchmarks to improve agent performance
- Ensure adherence to policies and standards
- Protect and defend against regulatory fines or legal action
- Quickly verify interaction outcomes, resolve disputes

As standard business practice, many organizations record some fraction of their calls, and almost without exception, recording begins as the call is connected to an agent or IVR, then finishes when the call is disconnected. For organizations who collect credit card information during a call, that information is now being captured during recording.

PCI DSS requires that cardholder data is protected — raising the question of how to reap the aforementioned benefits of call recording without unintentionally creating massive amounts of data (call recordings) that have the potential to jeopardize PCI compliance? Secure recording pause is one solution.

A secure recording pause occurs when the recording system is configured in a manner that pauses/stops the recording while the credit card and security numbers are being spoken or typed into a desktop application. The pause can be invoked either by an agent clicking a 'secure pause' button, which stops the recording for a pre-specified amount of time; or by provisioning the desktop where the recording is paused as soon as the agent begins entering data into the credit card field.

Though this type of solution will significantly reduce the number of recordings with cardholder data, it may not fully eliminate it, as it's dependent upon agent adherence to clicking the pause button and/or the credit card information being given within the timeframe of the pause.

And there's more to come…

The best way to handle PCI compliance may be to simply take it out-of-scope for the collector taking a payment. Recent solutions simply embed a payment vendor's Web services into the agent/collector desktop whereby credit card and cardholder information is entered directly into the payment vendor's system. In this scenario, the secure data is never captured within collector's system or database, though collection organization would still need to contend with agent exposure to that information during the transaction.

Partnering with service and technology vendors to ensure PCI compliance

Leading accounts receivable software and payment processing providers support tokenization, encryption and other solutions as part of a comprehensive strategy to reduce data exposure and mitigate fraud risks. In addition, they should be able to provide clients with PCI compliance documentation, including PCI compliance letters and PCI standard compliance checklists and templates. You are encouraged to query your vendors' PCI compliance practices in connection with their retention and periodic auditing of them.

Respecting Authority: Payment Authorization Requirements

With virtually no changes to Regulation E/Electronic Funds Transfer Act (EFTA) or National Automated Clearing House Association (NACHA) requirements for electronic check or debit card payment authorization in recent years, you would expect web, telephone and IVR-based collections to be business as usual. But while the rules remain the same, a changing regulatory environment suddenly has ARM organizations retracing their steps.

As agencies and their clients begin to face scrutiny and prepare for the prospect of Consumer Financial Protection Bureau (CFPB) supervision, some in the industry are reevaluating their credit/debit card and ACH collection strategies. While the following authorization guidelines should not in any way be construed as legal counsel, it does serve as the basis for best practices adopted by leading agencies who continue to manage payment transactions with confidence.

Authorization basics

Today, requirements for payment authorization get complicated because of the various methods of payment (ACH vs. debit), the collection medium (telephone, web, IVR, etc.) and the frequency of payment (single or recurring transactions). Each dimension factors into how consent, authentication and notification must be executed.

Guiding principles for payment authorization include:

a) **Being readily identifiable as an authorization.** Authorization must be explicit and clearly communicated to the consumer. The manner in which this occurs depends upon the method and medium of payment.
b) **Having clear and readily understandable terms.** A purported authorization that is not clear and readily understandable does not satisfy the authorization requirements of Regulation E. That means clearly communicating and documenting the 1) amount owed, 2) number of payments and 3) payment date.
c) **Providing that the Receiver may revoke the authorization only by notifying the Originator in the time and manner stated in the authorization.** Revocation rights must be afforded by the Originator and provide the consumers with reasonable opportunity to act on such revocation prior to the initiation of the entry. In other words, let the consumer know exactly how and under what conditions they may revoke their authorization. That means providing basic information like a telephone number to contact, business hours and the number of days the consumer has to revoke the authorization prior to payment processing.

ACH: double-checking your payment authorization requirements

NACHA, the governing association for the ACH network, maintains standards and guidelines for electronic check payments in much the same way that credit card companies do for credit/debit card transactions.

While NACHA and the credit card companies maintain guidelines, it is Regulation E, administered by the CFPB, that supervises federal regulations related to electronic payments — including both ACH and debit card transactions. Parts of Regulation E are recognized in both ACH and credit/debit card authorization standards. The following requirements and best practices apply to the various forms of collections for ACH payments under NACHA.

ACH authorizations: verbal and/or written consent

For telephone or w payment authorizations via ACH, extra care and attention must be paid to recurring transactions. Table 1 summarizes requirements for single and recurring transactions, whether for telephone, web or IVR.

	Agent/Telephone	Web	IVR
Single	Record verbal consent ***OR*** provide written notice prior to settlement date	Consent and authentication of consumer required. Written authorization through electronic signature	Verify identity, request and confirm payment terms with telephone pad key strokes Appropriate disclosures with response that indicates consent with the record containing consumer certified information
Recurring	Record verbal consent ***AND*** provide written notice, prior to settlement date	Consent and authentication of consumer required. Written authorization through electronic signature. Notice ***MUST*** also be provided to consumer	

Table 1: NACHA authorization requirements

Telephone recurring transaction payment authorizations may be the most problematic for agencies that follow the same procedures for both single and recurring transactions. As it applies to over-the-phone ACH transactions ("TEL" coded), the collector is obligated to either record the consumer's verbal consent or provide written notice, prior to settlement date, that the consumer confirms his/her oral authorization. Key note: the Devil lies in the "and" and the "or." For single transactions, the requirement is verbal consent OR written confirmation. For recurring transactions, you need BOTH verbal AND written authorization.

Although NACHA rules have certain provisions that appear to permit the use of audio recordings for authorization, federal law prohibits their use in the case of a consumer contract where consent is obtained electronically. It is Regulation E, with its reference to the E-Sign Act, which provides the federal paradigm pursuant to which electronic payments — including both ACH and debit cards — are processed. Compliance with the E-Sign Act is beyond the scope of this paper, so we recommend you consult your legal counsel.

Card Payments: Phone or Web Authorization Tips

For card transactions, the same principles outlined for ACH transactions apply, although there are some best practices that will ensure compliance and help to avoid potential disputes. The key here, again, is to authenticate the consumer and obtain consent.

Authentication for card transactions can be achieved using one of the following methods:

- Verification of address (AVS)
- Obtain CVVS/CVC2/CID information from the consumer card to validate that the card is in the possession of the consumer

The best approach, however, is the capture of BOTH. Keep in mind that collecting this authentication information bears its own risks. From a PCI compliance standpoint, collection agencies do not want to retain authentication information. As described earlier, this is where tokenization comes into play.

To prevent chargebacks and defend against disputes, it's highly recommended that collections agencies get the following information and include it on the sales draft, either via mail, email or fax:

- Cardholder's name
- Card account number, expiration date and CVVS/CVC2 Code (truncated or masked for security purposes)
- Billing address, including zip code

When handling card payments via the web, an approval code should be obtained and recorded for each and every attempted transaction.

In most cases, the greatest concern and source of ambiguity as it relates to payment authorization, whether via ACH or debit card, has been the issue of recurring payments. In the case of card transactions, recurring payments are valid, but it is recommended that these payments not go out farther than three months. An email or written letter notifying the consumer of each transaction will help to avoid disputes along the way.

With Convenience Comes Complexity: Convenience Fee Quandaries

Commonplace activities such as ACH, debit and credit card transactions for collections have come under additional scrutiny to ensure data security, proper authorization and disclosure. But other practices such as the permissibility of convenience fees have raised more fundamental questions about consumer rights and fairness. This strikes at the heart of the change in today's regulatory climate, where consumer advocacy is the order of the day.

For debt collectors, convenience fees represent an opportunity to lower operating costs and maximize revenues for themselves as well as their clients. The practice of collecting a "convenience fee" has been considered a common practice in the ARM industry. According to a 2013 insideARM.com/BillingTree survey, over 52% of clients or agencies are charging a convenience fee.

In some cases, agencies have collected fees from the consumer to help cover operating costs associated with alternative forms of payments, in exchange for the convenience of a simple, effective payment method. In other cases, vendors (usually the payment processor) collect a convenience fee to cover the vendor's transaction processing costs, with the agency recognizing no direct economic benefit.

As consumers continue to become more educated and are provided with more ways to lodge complaints (such as the CFPB Complaint Database), convenience fees may pose a greater risk for litigation, with greater risks of agencies getting on the CFPB radar.

For agencies issuing convenience fees today, the key is to understate each state's statutes and to stay close to upcoming state legislation.

At the center of an ongoing debate: who pays?

Who pays for electronic transactions has been a fiercely debated (and litigated) issue since the advent of digital payment processing. The question came to a head in 2010, when the Durbin Amendment mandated drastically lowered swipe fees on debit cards issued by banks with assets of $10 billion or more. As a result, big banks began to look for ways to recoup lost swipe fee revenues by passing new costs on to consumers. One example was Bank of America's short-lived attempt to apply a $5 monthly fee to its debit card-using customers. Consumer backlash from BofA's initiative resulted in actions like "Bank Transfer Day," where consumers were urged to transfer their bank accounts to not-for-profit credit unions.

While consumers were in revolt, major banks were fighting a years-long battle on another front against Visa/MasterCard over transaction fees. In 2005, JP Morgan, Chase, and Bank of America sued Visa and MasterCard, accusing them of anticompetitive practices in payment processing. The case was settled in 2012 for a total of $7.2 billion, comprising in a payment of $5.2 billion by Visa and MasterCard, and an agreement to reduce processing transaction fees for a period of eight months. In addition, the settlement allowed merchants to impose credit card surcharges under the terms of Visa/MasterCard's operating regulations.

The 2012 settlement did little to settle the matter of who pays for debit/credit card transactions or how they should be assessed. While the 2012 settlement allowed for the imposition of surcharges by merchants, for example, a number of states already had credit card surcharge bans in place and others have new legislation pending to ban this practice.

At the same time, major retailers were among the most vocal opponents to the settlement, as a statement on Walmart's web site suggests: *"The proposed settlement would not structurally change the broken market or prohibit credit card networks from continually increasing hidden swipe fees, which already cost consumers tens of billions of dollars each year."*

Regulations and guidelines: what is "convenience?"

Amidst this ongoing debate about "who pays for convenience?," the Fair Debt Collection Practices Act defines the law for anyone collecting debt. According to the FDCPA, an agency or third party can assess a convenience fee on debit card or credit card transactions, so long as:

- State laws permit it, and
- A convenience fee is expressly authorized in the underlying debt agreement.
- In addition, the card association rules state that at least one alternative payment channel is available, and is clearly disclosed.

The availability and disclosure of alternatives is critical to ensuring compliance, as one debt buyer and one debt collection law firm in Mississippi recently discovered. In March 2013, the Federal Trade Commission reached an $800,000 settlement with two firms who charged convenience fees to consumers who made payments over the phone, but failed to identify that payments could be made by mail or via a web site without incurring the convenience fee.

One fundamental question that has not been adequately addressed by these guidelines is **"what is a convenience fee — and how is it different than a surcharge?"** For guidelines, ARM organizations can look to rules issued by Visa/MasterCard, which apply to all "merchants" submitting transactions. According to Visa/MasterCard guidelines, a surcharge is applied for any use of a credit card or debit card. A convenience fee applies to a specific subset of transactions in which:

- Payment is not made in person (e.g., the transaction is processed as a "card not present" charge)
- It reflects a fee for a convenient, alternative form of payment
- A convenience fee is
    - a flat fee, assessed regardless of the value of the payment due
    - assessed equally across all types of payments (regardless of credit card/debit card issuer)
    - included as part of the total amount of the transaction

Traditionally, convenience fees could not be assessed on recurring payments, nor could they be assessed by third parties. The January 2013 "Visa Operating Regulations to Support the U.S. Merchant Litigation Settlement," however, do not expressly allow — or prohibit — the application of convenience fees for recurring payments. Likewise, while the operating regulations clearly define the authority for merchants to apply a convenience fee, the language with regard to a third party charging a fee on behalf of an agency is ambiguous.

"Void where prohibited by state or local law"

Although convenience fees assessed in connection with consumer debt are not governed directly by federal law, the climate in a growing number of states leans towards prohibiting passing along credit card surcharge fees to consumers.

As of March 2013, 10 states[3] maintain laws prohibiting retailers from imposing surcharges when consumers use credit cards. According to The American Banker[4], 18 more states were considering legislation — including Arkansas, Hawaii, Illinois, Indiana, Kentucky, Maryland, Michigan, Missouri, Nevada, New Jersey, New Mexico, Pennsylvania, Rhode Island, South Carolina, Tennessee, Utah, Vermont and West Virginia.

> …debt collectors will need to continue to keep an eye out for new legislation while looking for reinterpretations of existing laws.

With states continuing to scrutinize the imposition of fees upon consumers based upon their payment method, debt collectors will need to continue to keep an eye out for new legislation while looking for reinterpretations of existing laws.

Risky business

Today, convenience fees and surcharges represent the most ill-defined and most contentious practice among merchants and their third party representatives. With federal, state, credit card and bank stakeholders continuing to sort through the issues, it is more critical than ever that accounts receivable management companies assess and monitor their risks with regard to convenience fees. Because laws and standards remain in flux, it's not enough to establish policies and then monitor for compliance. Policies must be evaluated continuously, with revisions to procedures according to changes in federal, state or local laws, as well as bank or credit card guidelines.

[3] American Banker, Feb 13, 2013
[4] American Banker, April 1, 2013

Drawing Conclusions

While the benefits of offering multiple forms of payments across multiple media far exceed the risks, the reality is that the burden of compliance is increasing for anyone collecting payments from consumers. The old rules are now subject to new interpretations. Conflicts among the various levels of government, banks, credit card companies, NACHA and consumers continue to be contested in courtrooms across the nation. Standards for data security continue to be tested by the ingenuity and determination of criminals worldwide, resulting in new risks and new standards.

For ARM organizations, there are potential solutions to explore such as tokenization, secure IVR and encrypted screen recordings. It's also prudent to examine potential new revenue streams with things such as convenience fees, though it demands staying on top of the constant shifts in federal and state regulations. In the end, the best course of action is to rally internal resources on a consistent basis; leverage professional relationships to exchange knowledge and share best practices; and remain diligent and informed regarding changing regulations.

The proven leader in on-demand payment processing, BillingTree empowers customers with competitive advantage through a simplification of the billing and receivables process. By delivering the most innovative technology while making it as easy and inexpensive as possible to accept payments, BillingTree has revolutionized the payments landscape. Our software-as-a-service (SaaS) model delivers industry-leading payment solutions, proven integration, and point-and-click simplicity. BillingTree's focus on innovation has allowed us to help more than 1,200 customers eliminate manual processes and automate their payment cycles. BillingTree — Your Growth is our Business. For more information, visit www.mybillingtree.com or call 877.4.BILLTREE.

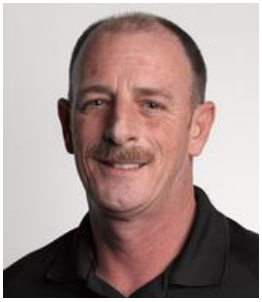
insideARM.com provides the most credible platform for service providers to reach potential clients, and is also uniquely qualified to help ARM businesses with their own websites, social media programs, and overall marketing strategies. With more than 75,000 subscribers, our website and newsletters reach collection agencies and law firms, debt buyers, creditors, suppliers of technology and services to these groups, regulators, industry investors, and many other interested parties.

Interactive Intelligence is a global provider of contact center, unified communications, and business process automation software and services designed to improve the customer experience. A core vertical focus of the company is Accounts Receivable Management. To improve the collections process, Interactive provides intelligent outbound dialing solutions with the tools needed to increase agent utilization and right-party contacts, eliminate workforce segmentation, implement the latest collection strategies in-house, and maintain compliance. This comprehensive functionality leads to faster, more effective debt collection and portfolio recovery. Overall, the company's standards-based, all-in-one IP communications software suite, which can be deployed via the cloud or on-premises, is in use by more than 6,000 organizations worldwide, including hundreds of firms in the ARM industry. Interactive Intelligence was founded in 1994 and is headquartered in Indianapolis, Indiana, U.S.A. with offices throughout North America, Latin America, Europe, Middle East, Africa and Asia Pacific.

The Authors

Chris Gonzales is BillingTree's Director of Products and Services and is responsible for the development and execution of the product portfolio growth strategy.

Prior to BillingTree, Chris served as the global Vice President of Sales and Marketing for MedAire, an integrated medical and security services provider. Chris was responsible for global sales, channel and marketing strategies, including the development of new products and services for the aviation and maritime markets. Previously, Chris served as a Product Portfolio Leader at Johns Manville, a building materials manufacturer, and as a Strategic and Product Marketing Manager at Honeywell Aerospace. Chris has a degree in finance from Arizona State University and an MBA from Northwestern University's Kellogg School of Management.



Ian Winder is the Product Manager for the Accounts Receivable Management (ARM) vertical at Interactive Intelligence. This concentration started October 2010, with the acquisition of Latitude Software, a leading provider of ARM software solutions. As the Latitude product manager, he is responsible for determining the optimum methodology and approach for leveraging both companies' capabilities in the ARM industry.

Ian began his career in the ARM industry in 1986 as a senior technology leader for multiple collections and debt purchasing organizations; most recently as CIO then CTO at Risk Management Alternatives, and as SVP of Information Services at West Asset Management.