

INSIDE: Noteworthy <i>ACH Rules</i> Updates.....	pg. 1
NACHA Joins Microsoft, FS-ISAC and Others in Unprecedented Cross-Industry Effort to Disrupt Massive Cybercrime Operation.....	pg. 1
Whitepaper Analyzes Mobile Payment Impact on Consumer Shopping and Purchasing Habits.....	pg. 3
Android Malware is Fastest-Growing Category in IT	pg. 4


Bill Payment Exceptions Cost Industry \$720 Million Annually	pg. 4
Remote-controlled Android Malware Hijacks Tokens.....	pg. 5
Retailer Interchange Settlement Prompts Removal of No-Surcharge Rule	pg. 5
CFPB's First Significant Enforcement Action Will Cost Capital One \$210 million	pg. 7
CFPB Launches Controversial Complaint Website.....	pg. 7

Noteworthy *ACH Rules* Update

The *ACH Rules* are continuously evolving to mesh with the fast-paced environment of the payments industry. This article highlights recent *ACH Rules* ballot issues and rule implementations. What do these changes mean to you?

Recently Implemented *ACH Rules* Change That Affect Originators

Dishonor of Return Entries

This amendment modifies the *ACH Rules* to eliminate the requirement that the ODFI or Originator must have suffered a loss before being able to dishonor a return as untimely. 

**EPCOR Payments
Conference -
Spring & Fall 2013**

May 14 - 16
Columbus, OH

October 28 - 30
Overland Park, KS

SAVE THE DATE

NACHA Joins Microsoft, FS-ISAC and Others in Unprecedented Cross-Industry Effort to Disrupt Massive Cybercrime Operation

In its most complex effort to disrupt botnets to date, Microsoft Corp., in collaboration with the financial services industry—including the Financial Services—Information Sharing and Analysis Center (FS-ISAC) and NACHA—*The Electronic Payments Association*—as well as Kyrus Tech Inc., recently announced it has successfully executed a coordinated global action against some of the most notorious cybercrime operations that fuel online fraud and identity theft. With this legal and technical action, a number of the most harmful botnets using the Zeus family of malware worldwide have been disrupted in an unprecedented, proactive cross-industry action against this cybercriminal organization.

Through an extensive and collaborative investigation into the Zeus threat, Microsoft and its banking, finance and technical partners discovered that once a computer is infected with Zeus, the malware can monitor a victim's online activity and automatically

start keylogging or recording a person's every keystroke, when a person types in the name of a financial institution or ecommerce site. With this information, cybercriminals can steal personal information that can be used for identity theft or to fraudulently make purchases or access other private accounts. In fact, since 2007, Microsoft has detected more than 13 million suspected infections of the Zeus malware worldwide, including approximately 3 million computers in the United States alone.

"With this action, we've disrupted a critical source of money-making for digital fraudsters and cyberthieves, while gaining important information to help identify those responsible and better protect victims," said Richard Boscovich, senior attorney for the Microsoft Digital Crimes Unit. "The Microsoft Digital Crimes Unit has long been working to combat cybercrime operations, and today is a particularly important strike against cybercrime that we expect will be felt across the criminal underground for a long time to come."

see **CYBERCRIME** on page 2

CYBERCRIME continued from page 1

This disruption was made possible through a successful pleading before the U.S. District Court for the Eastern District of New York, which allowed Microsoft and its partners to conduct a coordinated seizure of command and control servers running some of the worst known Zeus botnets. Because the botnet operators used Zeus to steal victims' online banking credentials and transfer stolen funds, FS-ISAC and NACHA joined Microsoft as plaintiffs in the civil suit, and Kyrus Tech Inc. served as a declarant in the case. Other organizations, including F-Secure, also provided supporting information for the case.

As a part of the operation, on March 23, Microsoft and its co-plaintiffs, escorted by the U.S. Marshals, seized command and control servers in two hosting locations, Scranton, Pa., and Lombard, Ill., to seize and preserve valuable data and virtual evidence from the botnets for the case. Microsoft and its partners took down two Internet Protocol addresses behind the Zeus command and control structure, and Microsoft is currently monitoring 800 domains secured in the operation, which are helping identify thousands of computers infected by Zeus.

This is the second time Microsoft has conducted physical seizures in a botnet operation, and it is the first time other organizations have joined Microsoft as plaintiffs in the legal case for a botnet operation. This is also the first operation for Microsoft that involved the simultaneous disruption of multiple operating botnets in a single action and is the first known time the Racketeer Influenced and Corrupt Organizations (RICO) Act has been applied as the legal basis in a consolidated civil case to charge all those responsible in the use of a botnet.

"As crimes against banks and their customers move from stickups to mouse clicks, we're also using our own mouse clicks—as well as the law—to help protect consumers and businesses," said Greg Garcia,

a spokesperson for the three major financial industry associations that worked with Microsoft on this initiative.

"Disrupting the Zeus botnets is just one strike in our long-term commitment to help defend and protect people."

Because of the complexities of these targets, unlike Microsoft's previous botnet operations, the goal of this action was not to permanently shut down all impacted Zeus botnets.

However, this action is expected to significantly impact the cybercriminals' operations and infrastructure, advance global efforts to help victims regain



control of their infected computers, and also help further investigations against those responsible for the threat. As with its previous botnet operations, Microsoft will now use the intelligence gained from this operation to partner with Internet service providers and Community Emergency Response Teams around the world to help rescue people's computers from the control of Zeus, helping to reduce the size of the threat that these botnets pose and to help make the Internet safer for consumers and businesses worldwide.

Together, these aspects of the operation are expected to undermine the criminal infrastructure that relies on these botnets

every day to make money and to help provide new tools for the industry to work together to proactively fight cybercrime. Michael Tanji, chief security officer of Kyrus Tech Inc., who helped analyze the Zeus malware and determine which botnets were the most dangerous said, "We are proud to have played a part in this groundbreaking effort and hope that others will start working together to combat malicious activity at the same scale as it is being perpetrated."

There are steps consumers and businesses can take to better help protect themselves from becoming victims of malware, fraud and identity theft. All computer users should exercise safe practices, such as running up-to-date and legitimate computer software, firewall protection, and antivirus or antimalware protection. People should also exercise caution when surfing the Web and clicking on ads or email attachments that may prove to be malicious.

For computer owners worried their computers might be infected, Microsoft offers free information and malware cleaning tools at support.microsoft.com/botnets that can help people remove Zeus and other malware from their computers. For businesses looking for more information about corporate account takeover issues, including those due to malicious software, a fraud advisory from FS-ISAC, the FBI and the U.S. Secret Service can be found at www.fsisac.com/files/public/db/p265.pdf.

More information about today's news and the coordinated action against Zeus is available at www.microsoft.com/presspass/presskits/dcu.

Legal documentation in the case can be found at www.zeuslegalnotice.com.

Click [here](#) to view EPCOR's recent *Fraud Alert* on this subject. 🟢

Source: NACHA

WE'RE GEARING UP FOR PAYMENT SYSTEMS UPDATE!

Learn EVERYTHING you
need to know about:

- Impacts of new ACH Rules
- Emerging Technologies
- Regulatory Updates
- Risk and Fraud Concerns
- Payment Systems Initiatives
- Remotely Created Checks
- Healthcare Payments
- Global Payments

ARE YOU UP-TO-DATE ON
PAYMENT SYSTEMS RULES
& REGULATIONS?

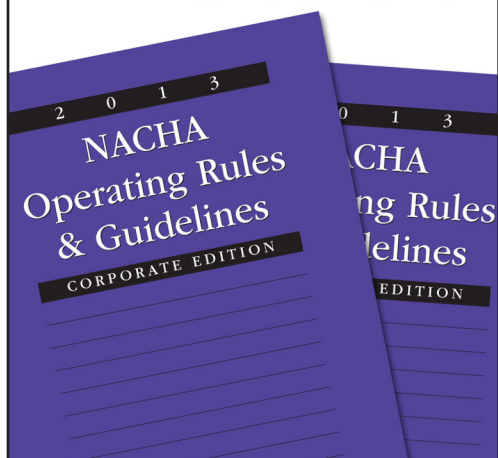


VISIT EPCOR.ORG TO
FIND WHICH OF THE
50+ LOCATIONS
IS NEAREST YOU.

PRE-ORDER YOUR 2013 ACH RULES TODAY!

RELYING ON OUTDATED
VERSIONS CAN BE CONFUSING
AND HURT COMPLIANCE.

CURRENTLY TAKING
ORDERS IN THE
ONLINE STORE AT
WWW.EPCOR.ORG



Whitepaper Analyzes Mobile Payment Impact on Consumer Shopping and Purchasing Habits

New research from Parks Associates finds that over 50 percent of United States broadband households want the ability to scan barcodes for product price and

mobile payment technologies, including the emerging Near Field Communication (NFC)-based retail mobile wallet solutions, processed over \$10 billion in transactions in



promotional information on their next mobile phone. The international market research firm's new whitepaper "Mobile Payment—Stepping into Uncharted Territory," reports 37 percent of U.S. mobile phone owners find the mobile wallet concept appealing, with interest highest among younger households and smartphone owners.

"For consumers, the most attractive benefit of mobile payment apps is they reduce the number of credit cards they have to carry," said Harry Wang, Director, Mobile and Health Research, Parks Associates. "The mobile phone is the main device people use to organize their lives, and mobile payment solutions offer significant conveniences, including organizing receipts and eliminating the need to carry cash."

"Mobile Payment—Stepping into Uncharted Territory" reports that various

2011 in the North American market alone. The whitepaper highlights new types of mobile payment technologies and solutions and analyzes current and future benefits to consumers, mobile carriers, small and medium businesses, mobile app and solution developers and brick-and-mortar retailers.

Currently, 50 percent of United States broadband households own a smartphone, and 80 percent of United States mobile phone users have a web browser on their mobile handset. Mobile payment, or mPayment, is the purchase of goods or services for which a mobile phone is used in the payment process, either in person, in a retail store or remotely, using mobile broadband access or cellular network infrastructure.

[Download](#) the whitepaper.

Source: *Pymnts.com*

Android Malware is Fastest-Growing Category in IT

There's good news on the mobile-malware front, but only if you're in the mobile malware business: Not only did the number of attacks on mobile devices of all kinds grow by 155 percent compared to 2010, Android, increased the number of its available viruses, Trojans and other malware at the unheard-of rate of 3,325 percent according to a report from Juniper Networks.

German testing lab AV-Test makes the estimate a little more precise, avoiding the question of how to calculate the growth rate in percentages when starting from zero: In January 2011 testers were able to collect almost no malware in the wild that was tailored specifically to Android. By the end of February 2012 the catalog of Android malware apps had grown to nearly 12,000.

More good news (if you write or distribute malware for a living): After testing 41 antivirus/antimalware apps that run on Android, AV-Test concluded that barely a third performed adequately and almost none lived up to the standards most users would expect of a standard antivirus product for PCs.

The best-performing Android antivirus products detected more than 90 percent of the malware AV-Test tried to slip past them – still lower than mid-90-percent and upward rated by the best antivirus products on PCs or Macs.

Best-performing AV apps—>90% success rate: Avast, Dr. Web, F-Secure, Ikarus, Kaspersky, Zoner and Lookout.

Products described by AV-Test as “still very good” detected between 65 percent and 90 percent of the malware present.

Second-best mobile AV apps— 90% to 65% success rate: AegisLab, Super Security, AVG, Bitdefender, ESET, Norton/Symantec, QuickHeal, Trend Micro, Vipre/GFI and Webroot.

The rest don't bear investigation because, even if they are working well on your particular device, they don't work well enough to make every mobile user safer. Catching between 40 percent and 65 percent of malware attacks is a lot better than catching none of them. However, it also brings the success rate down below the margin of error.


Using one of those apps, if your phone starts speaking in tongues, projectile-vomiting pea

soup and rotating its front-facing camera all the way around to face back and then back around until it's facing you again, you still couldn't rely on the antivirus to tell you if the phone was infected or possessed.

Third-tier mobile AV apps—40% to 65% “success:” Bullguard, Comodo, G Data, McAfee, NetQin and Total Defense.

Among the biggest weaknesses for the worst-performing apps was the ability to scan installed apps and important files rather than all the storage connected in any way to the device. Without scanning SD cards and other storage, AV scans missed malware hiding in malicious APK files (self-installing executables) and waiting for the opportunity to take over.

Even the effective scans varied widely in their ability to pick up specific families of malware, which is important because some families are prevalent in one geographic area and missing completely in others.

Whatever you do, don't download anything. Or click on anything. Or turn on your phone without dunking it in bleach or hot, soapy water first. 

Source: ITWorld

Bill Payment Exceptions Cost Industry \$720 Million Annually

On May 1, 2012, NACHA and its Council for Electronic Billing and Payment (CEBP) released results of a study that documents volume, causes and costs of bill payment exceptions across several payment channels. The [2012 Exceptions Benchmarking Study](#) reveals that 0.58 percent of total bill payments (including checks, ACH, cards and cash payments) in 2011 were not able to be posted accurately upon receipt by billers. Based on this exception rate, it is estimated that 130 million payments required exception handling, costing the industry approximately \$720 million.

The 2012 report, a follow up to a 2007 study that exclusively measured online banking bill payments, further reveals that the overall exception rate in the online banking channel increased from 0.4 percent in 2007 to 0.51 percent in 2011.

“Although the percentage of exceptions may appear inconsequential, volume is high, and the impact on billers, processors, financial institutions, small businesses and even consumers is significant,” said Kathy Romano, Director of Payment Processing for Verizon's landline customer business and member

of CEBP. “Exceptions require someone to manually resolve issues, creating additional expense for corporations and processing organizations. More importantly, consumers' payments will be delayed in processing, sometimes resulting in late fees or even service impacts.”

“Consumers and businesses alike want convenient, versatile and secure payment options,” said Janet O. Estep, president and CEO of NACHA. “As such, a growing number of businesses and consumers are making the conscious decision to use electronic payments

see EXCEPTIONS on page 5

EXCEPTIONS continued from page 4

such as Direct Deposit via ACH and Direct Payment via ACH. To continue to meet the needs of these businesses and consumers and retain confidence in electronic payments systems, it is important that we work to reduce exception volume.”

According to the study, a major cause of exceptions across all bill payment channels is missing or invalid consumer account numbers with their billers. For billers, this error is the leading cause of exceptions. For processors, missing or invalid account numbers is the second leading cause of exceptions, with processing differences topping the list.

In order to help reduce the number of bill payment exceptions, sharing information, standardizing processes and educating consumers is critical. Study findings indicate that more than one-third of processors do not receive required information from billers to verify account numbers and masks, which

define the format for a valid account number. Requiring that mask edits be applied prior to payment origination is a key procedure for reducing exceptions, but this practice is not universally applied. Additionally, the study reveals there is a lack of standard procedures to follow when a consumer enters an incorrect account number. Some processors notify the consumer, others attempt to make an edit, while others resort to sending a paper check. Although most billers stated they provide consumers with information and systems to help them include accurate account information when paying the biller directly, the majority reported they do not provide this same service for consumers paying through a bank or bill payment provider.

“This study demonstrates how important sharing information and standardizing processes is to reducing bill payment exceptions,” said Chris Huppert, chair of CEBP and Senior Vice President, Wells Fargo. “It also underscores the value of programs such as

EBIDS (Electronic Bill Information Delivery System), which requires bill payment originators to apply account edits provided by the biller before originating a payment. By enforcing edit rules, EBIDS improves efficiencies and ultimately reduces bill payment exceptions.”

The CEBP recommends specific strategies to help mitigate the number of bill payment exceptions. In addition to using services such as EBIDS for standardization purposes and to ensure account masks are being used and shared, the CEBP suggests the following:

- Developing directories/shared databases to verify account numbers, structures and billing/remittance details
- Enhancing communications among billers, banks and processors, especially for resolving exceptions
- Increasing available options to correct or validate account numbers by sharing scrub files and/or master account files.

[Download](#) the 2012 Exceptions Benchmarking Study results. 📄

Remote-controlled Android Malware Hijacks Tokens



Security researchers at McAfee have discovered a malicious Android application capable of grabbing banking passwords from a mobile device without infecting the user's computer.

The latest piece of Android Malware, dubbed FakeToken, contains man-in-the-middle functionality to hijack two-factor authentication tokens and can be remotely controlled to grab the initial banking password directly from the infected mobile device.

[see ANDROID on page 6](#)

Retailer Interchange Settlement Prompts Removal of No-Surcharge Rule

Visa and MasterCard recently announced that they, along with several major issuers, reached a \$7.25 billion class-action settlement with U.S. merchants. In addition to being party to the largest monetary antitrust settlement in U.S. history, the networks agreed to permit retailers to impose a surcharge on credit transactions subject to a cap and a level playing field with other general purpose card competitors.

Previously, the no-surcharge rule (NSR) had been a staple for both MasterCard and Visa, ultimately prohibiting merchants from charging consumers more to pay with credit cards. Merchants claim that because of the NSR, all consumers, regardless of their payment method, incurred higher costs. Now, in theory, merchants should be able to

lower their prices and pass along the costs of a credit card transaction only to those consumers paying with a credit card.

However, in some countries where surcharging has been allowed, merchants have used checkout fees as a profit source. The Reserve Bank of Australia was recently forced to cap the amount that retailers could charge in order to prevent merchants from taking advantage of consumers. Luckily, the Visa and MasterCard settlement does include some safeguards that could help curb any abusive or excessive surcharges:

- Merchants are only allowed to assess a fee that is equivalent to what they pay to accept credit cards—which in the U.S. is typically between 1.5%-3%.

[see SETTLEMENT on page 6](#)

ANDROID continued from page 5

As explained by McAfee's Carlos Castillo, the malicious application targets specific well-known financial entities by posing as a Token Generator application. Upon installation of the application, the malware utilizes the logo and colors of the financial institution in the icon of the application, making it appear more credible to the user.

When the application executes, a WebView component displays an HTML/JavaScript web page pretending to be a Token Generator. The web page also appears to be from the targeted financial institution (same variant of the malware but with different payload).

To obtain the fictitious token, Castillo discovered that the user must enter the first factor of authentication (used to obtain initial access to the bank account). If this action is not performed, the application shows an error.

"When the user clicks "Generar" (Generate), the malware shows the fake token (which is in fact a random number) and sends the password to a specific cell phone number along with the device identifiers (IMEI and IMSI). The same information is also sent to one of the control servers along with further data such as the phone number of the device. The malware finds the list of control servers from an XML file inside the original APK," he added.

Castillo found that the FakeToken app can also hijack the list of contacts stored in the device (name and number) and contains commands to update itself or spy on the infected machine.

Android malware that targets financial entities is in constant evolution. Man-in-the-middle attacks are just the beginning. We now see more sophisticated, remote-controlled banking Trojans that can get more than one factor of authentication and even modify a phishing attack to obtain other required credentials (such as the name or the ID number of the user), which will be utilized to perform electronic fraud. Due to the increasing popularity of Android and mobile-banking applications, more threats like this are likely to appear. 📍

Source: ZDNet; Ryan Naraine

SETTLEMENT continued from page 5

- Consumers can only be charged checkout fees for credit card usage. Merchants cannot charge customers for the use of their debit card.
- Merchants must provide "clear disclosure" of any checkout fees at their store entry and at the point of sale or on their first page if it is an online environment.
- The disclosure must list the amount of the surcharge, that the charge is being imposed by the merchant and that the surcharge is not greater than the costs merchants pay to accept cards.
- Merchants must provide "clear disclosure" of the dollar amount of the checkout fee on the transaction receipt.

Also, [10 states](#) with 40 percent of the U.S. population (including California, Florida, New York, and Texas) currently prohibit retailers from charging customers a fee for using a credit card. Residents of these states should report any evidence of retailer checkout fees to their state attorneys general.

Only time will tell if merchants will actually lower their prices and pass along the costs of a credit card transaction only to those consumers paying with a credit card. In the payment card market, theory and practice often differ. The Durbin Amendment, in theory, was intended to benefit consumers, assuming that merchants would pass along their savings through lower prices. However, the debate continues on whether merchants who received interchange relief (some actually experienced increased rates and are in fact passing along these costs to consumers) are really passing on the savings.

Another debate surrounding whether the consumer actually benefits is most likely headed our way. Will many merchants actually choose to impose a surcharge on credit-card-paying consumers? Will the surcharging merchants actually drop prices from their current levels or simply add a surcharge on



top of existing prices? Will networks lower the effective interchange rates thus making it less costly for consumers to use credit cards should merchants choose to actually surcharge?

Will credit card surcharging take place in the United States?

In theory, the surcharging provision seems like a win for merchants, but in practice, will the surcharge provision have any impact at the point of sale? And what will prevent surcharging from being put into widespread practice in the United States?

Keeping in mind the backlash that one bank experienced when it proposed a new debit card fee, will any merchant that attempts to implement a surcharge (actual implementation of a surcharge with various types of cards and payment environments is worthy of an entire discussion itself) face similar scrutiny?

If a merchant chooses to charge consumers a fee for using a credit card, would the fee and the merchant then fall under the authority of the Consumer Financial Protection Bureau?

With so many questions to be answered, one thing is certain—The surcharging debate around this settlement and ultimate outcome will no doubt be interesting moving forward. 📍

Source: *Portals and Rails, Atlanta Fed Retail Payments Risk Forum, Douglas A. King; Electronic Payments Coalition*

CFPB's First Significant Enforcement Action Will Cost Capital One \$210 million

Capital One Bank NA will pay out \$210 million in fines and penalties following the Consumer Financial Protection Bureau's determination that the bank was engaging in deceptive marketing tactics.

According to the CFPB, Capital One's sales network was pressuring and misleading customers into buying so-called add-on products like payment protection and credit monitoring at the time of card activation. We are putting companies on notice that these deceptive practices are against the law and will not be tolerated, said Director Richard Cordray in a statement.

Capital One has not admitted any wrongdoing, and the announced payouts are part of a settlement agreement. Its official statement reads: Capital One's third party vendors did not always adhere to company

sales scripts and sales policies for Payment Protection and Credit Monitoring products, and the bank did not adequately monitor their activities.

We are accountable for the actions that vendors take on our behalf," said Ryan Schneider, President of Capital One's Card business, in the statement.

The \$210 million payout Capital One is now responsible for will end up with three different parties: \$140 million will be paid to consumers in the form of refunds; \$25 million goes to pay a fine levied by the CFPB; and \$35 million is for a fine charged by the Office of the Comptroller of the Currency.

An estimated two million consumers will receive some form of refund from Capital One, the CFPB says, either as a credit on current account statement or via check.

Capital One says consumers will begin receiving refunds later this year.

If the CFPB decides to further pursue other banks that sell such products, more refunds and penalties may be on the way. This practice is hardly limited to Capital One, said Philadelphia lawyer Richard Golomb in an interview with the New York Times. Indeed, Bloomberg reports that the CFPB and FDIC have already subpoenaed other issuers regarding related subjects.

Capital One has likely been on the CFPB's radar since the agency began collecting financial services complaints from consumers. In its first annual report, roughly 16 percent of the complaints filed by consumers were tied to Capital One accounts, representing roughly 2,700 filings between July 21, 2011, and May 15, 2012, the most of any issuer. 🟢

CFPB Launches Controversial Complaint Website

The Consumer Financial Protection Bureau (CFPB), in the face of heated controversy and vocal opposition from the financial industry, launched a website that allows consumers to browse through complaints filed against large financial companies.

Website users can see the name of the company targeted by each complaint, the nature of the issue, the company response—including timeliness—and the zip code of the complainer. Users can also generate charts showing which banks attract the most complaints, which issues are hardest to resolve and which regions of the country seem the most saturated with complaints.

"(This) is a major milestone for consumers and all those who are interested in knowing more about their day-to-day experiences," said Richard Cordray, the bureau's first director. "We believe this is the first time that

the general public has been able to see such individual-level consumer complaint data for financial products and services. ... Anyone with access to the web will be able to review and analyze the information, and draw their own conclusions."

Initially, the website will only include a small fraction of the 17,000 complaints filed regarding credit cards since July of the last year, when the agency began receiving customer gripes. For the time being complaints listed are limited to those filed since June 1, as the agency works out the kinks in its "beta" launch of the database.

A change in the way the agency categorizes resolutions has forced the agency to limit the initial release, said an agency official, speaking on background. Older complaints are being re-categorized and will be added to the public database by the end of the year, the official said.

Complaints about mortgages and checking accounts will also be added later, making Tuesday's launch a bit of a baby step toward providing full complaint access to consumers.

The financial industry has expressed concern surrounding the launch. Since the complaints represent raw, unverified data that could be misleading, many feel the release of the data is unfair.

"Bureau publication of complaint data alone implies an official endorsement of inferences drawn out of context and suggests reliability about overall issuer customer experience and satisfaction that is not well-founded and that invites untrustworthy analysis that will mislead consumers," said the American Bankers Association in its public comments on the consumer bureau's proposal to publish the data.

see [WEBSITE](#) on page 8

The bank lobbying group also complained that publication of unverified complaints is at odds with the bureau's mission to be a data-driven banking regulator.

"The Bureau's proposal expands its role by inventing a new mission of publicly outing information about an issuer's customer experience and satisfaction record, a function that is fundamentally at odds with its obligation to handle confidentially supervisory information," it said.

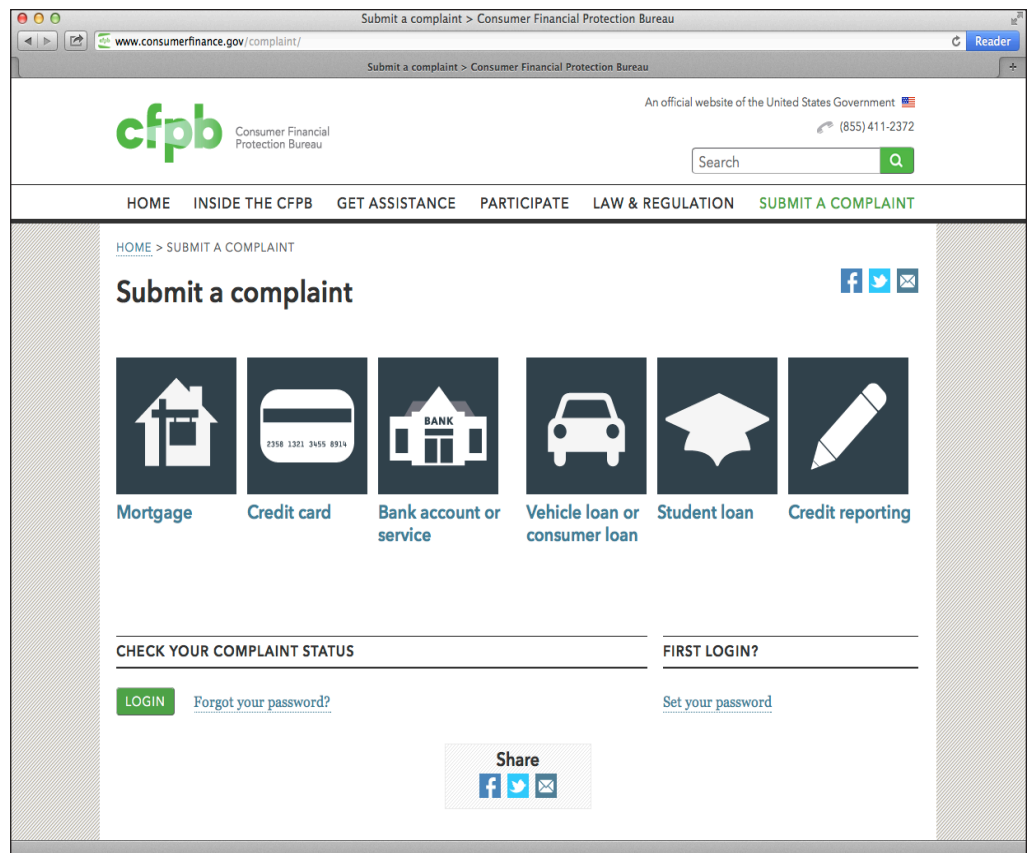
Other financial industry officials have compared public release of the data to gossip, and the database to the customer review site Yelp.com, complaining that many consumer complaints are unfounded, and some are fraudulently posted by competitors.

But the bureau official said each individual complaint was a worthy data point that consumers should consider when weighing decisions on banking products, and that release of the data would give banks an incentive to compete on customer service.

The agency will confirm that an authentic business relationship exists between complainer and target, however nothing else about the complaint will be verified. A warning will tell users that accuracy of the information has not been confirmed, according to the agency official. Complaints will only appear after a bank has responded, or until the 15-day response period has expired. Also, the agency will not offer opinions on the meaning of the data, the official said.

Initially, the "narrative" section of the complaints will not be published, because the agency has not yet determined how to sanitize the information to avoid publishing personal information, which could be harmful to the consumer. In fact, Cordray stressed that none of the complainers' personal information will be published.

Most government complaint data is not public, a situation which has drawn criticism in the past from consumer advocates.



The Federal Trade Commission, for example, collects hundreds of thousands of complaints from consumers but only makes the information available in aggregate, or when it files litigation against a firm. Because only a tiny fraction of complaints lead to litigation, the possibility exists that consumers fall for scams or unfair business practices committed by firms that are already attracting a pile of complaints in a government database.

The consumer bureau's model aims to enable consumers with the ability to learn from each other, and avoid unfair treatment. The data will provide a real-time view of what's happening in the marketplace, the agency official said, and could prevent consumers from falling for new tricks or traps invented by the financial industry.

Still, even in the Internet age, where sites like Yelp.com that let consumers warn each other are common, sharing of complaints filed with government agencies is extremely controversial. Last year, the Consumer Product Safety Commission made its

complaints available for the first time at SaferProducts.gov. Almost immediately, an as-yet-unnamed firm filed a federal lawsuit to keep a complaint about an allegedly dangerous product off the public website.

Cordray stated he hoped publication of the data would make it easier for consumers to seek fair treatment from financial institutions.

"Nobody needs to be told there are deep problems in the consumer financial product marketplace—it is why we were created in the first place...For every consumer who reaches out to us to tell us about their troubles, we know that many others have the same troubles but suffer them in silence," Cordray said. "These complaints tell us personal stories of real pain. ... Do your own digging. Find your own information. And help us make the marketplace a better and safer place."

[Download](#) the CFPB's report—Consumer Response: A Snapshot of Complaints Received. 📄

Source: Bob Sullivan, *The Red Tape Chronicles*, MSNBC Blog



Electronic Payments Core of Knowledge

EPCOR is your electronic payments core of knowledge and influence. We are a member-focused association devoted to providing personalized support and services.

The mission of EPCOR is to provide financial institutions with reliable payments and risk management education, information, support and national industry representation.



Through our direct membership in NACHA, EPCOR is a specially recognized and licensed provider of ACH education, publications and support.

© 2012, EPCOR. All rights reserved.

www.epcor.org

3100 Broadway, Ste. 609, Kansas City, MO 64111

800.500.0100 | 816.474.5630 | fax: 816.471.7665