What’s inside

The dangers of social engineering .......................................................... 2
Falcon rules for EMV fallback transactions ........................................... 4
Join our biannual onFraud webinar in August ....................................... 5
Reminders when using SHAZAM Card Block ........................................ 6
New Easy PIN option: No reference numbers ....................................... 7
Hackers know your vulnerabilities; do you? ........................................... 9
New client support menu options ......................................................... 10
Make life easier using SHAZAM Web Rep fraud forms ........................... 11
Cardholders will show off custom debit cards; you’ll increase revenue .... 12
Helpful tips for SHAZAM Access Files tab upgrade ............................. 13
SHAZAM training .................................................................................. 15
‘Pampered Rewards’ winners ............................................................... 16
The dangers of social engineering

Know who you’re talking to

Social engineering has been a key component in many, if not most, of the successful business breaches in the news today. Attackers use a variety of techniques to learn enough about a target to successfully acquire login credentials, gain unauthorized access to a location or convince employees to transfer funds or data to the attacker.

How does an attack work?
Attacks will usually begin with the attackers performing reconnaissance of their target. They may search publically accessible company websites, social media sites (for example: LinkedIn® or Facebook®), or “dumpster dive” through trash to find the information needed. They may even take photos of or steal a badge to create a facsimile.

They could then make calls to switchboards or receptionists impersonating as an employee or vendor to gain further knowledge or access to the target.

With this knowledge, they may seek information about operations, such as when doors are unlocked, what time deliveries are expected, what access procedures are for visitors, etc.

Once the attackers have all the information they need for the particular scam they’re perpetrating, they put it to use. A couple examples include:

• Posing as an employee to convince a technical support person to change a password to one of their choosing

• Pretending to be a third-party service provider, such as an electrician, plumber or deliveryman, to gain physical access to mechanical rooms or office spaces

Attacks on senior members
In more recent cases, attackers compromise the email accounts of senior members of an organization. This is an attack called business email compromise (BEC).

They might use fixed information they’ve gained to take advantage of password reset features and gain access to an account. They may spoof an email address that looks like the company’s standard email format, but actually points to a third-party controlled account.

Once they do have control, they use other information to impersonate senior leadership. For example: If they have knowledge of the CEO’s schedule, they might wait to try a

—Continued on next page
scam until he or she is out of town. This could end in the attacker having an employee make an emergency transfer of funds into an account in the attacker's control.

Avoid becoming a victim
Unfortunately, the number of social engineering techniques is as high as the number of bad guys! Here are some steps to decrease your chances of being breached:

- Stay aware and knowledgeable on how to defend against current scams
- Maintain employee awareness regarding information security over the telephone or internet
- Educate all levels of employees to avoid posting personal or work-related information on publicly accessible sites
- Provide and enforce the use of two-factor authentication whenever possible
- Encourage your employees to be aware of their surroundings
  - If they don’t know if someone belongs, teach them to ask questions

- Implement secondary controls for sensitive tasks, such as password changes, money transfers, badge reissues, etc.

Cybersecurity assessment
The question many institutions may find themselves asking is, “Are we cybersecurity ready?” With SHAZAM Secure®, we can help answer that question for you. SHAZAM Secure is our very own cybersecurity assessment tool that’s easy to follow and complete, saving you valuable time and resources.

Once the assessment is complete, an inherent risk profile rating and maturity level will be provided so you can better understand where you are today relating to cybersecurity preparedness. Our team can also help you evaluate and review your current assessment to ensure your institution is staying ahead of the regulatory compliance curve.

For more information
If you have questions, please contact Jay Lohmann, SHAZAM’s senior GRC analyst, at 800-537-5427, ext. 4211.
SHAZAM fraud operations is pleased to announce we’ve created a successful rule to decline suspicious EMV® fallback transactions.

What is an EMV fallback transaction?
When a merchant is attempting to process an EMV card for payment and is unable to read the chip, they can “fall back” to reading and processing the card as a magnetic stripe transaction. If the transactions are approved, there may not be chargeback recourse for the financial institution.

This sometimes happens on valid transactions if the card is inserted incorrectly, or if somehow the chip has been damaged.

More likely, this will happen when a fraudster has made a counterfeit card with a valid, cloned magnetic stripe. He or she may make the card to appear to have a chip, and when it doesn’t work as a chip (EMV) transaction, the merchant will run it as a magnetic stripe transaction.

To avoid losses on fallback transactions, SHAZAM fraud operations has implemented the following FICO® Falcon® Fraud Manager rules for case creation and Falcon Real-time.

Falcon rules
The Falcon Case Create rule is:

Create case if transaction is EMV Fallback, no PIN, transaction is outside cardholder ZIP code range, merchant category code starts with “5,” transaction amount >=$50, Falcon score is >=430, and PAN is not on known travel notice.

The Falcon Real-Time Decline rule is:

Decline if transaction is EMV Fallback, no PIN, transaction is outside cardholder ZIP code range, merchant category code starts with “5,” transaction amount >=$50*, Falcon real-time score is >= the financial institution’s Falcon real-time threshold minus 400, and PAN is not on known travel notice.

* If not on Falcon real-time 100 percent scoring, transaction amount is >=$100.

As a reminder, a Falcon real-time decline (Action Code 102) will also create a Falcon case. When we refer to “outside the cardholder ZIP code range,” it means the state the cardholder lives in and all surrounding states.

We’ll continue to monitor the rules and make any changes as needed. The rules have been updated in the Fraud Watch section of SHAZAM Access.

Questions?
Please call SHAZAM fraud operations at 800-537-5427, ext. 2899.

Sign up
If your institution is not yet using 100 percent Falcon real-time scoring, now is the time to sign up! Talk to your client executive today.
Join our biannual onFraud webinar in August

The SHAZAM fraud operations department provides free webinars on a variety of fraud topics each year in February and August.

How to participate

From 10 to 11 a.m. CT on Aug. 10, 2016, we’ll host a SHAZAM onFraud webinar called “What’s a SHAZAM-identified compromise?” As a side topic, we’ll also review a new global FICO® Falcon® Fraud Manager rule that’s been created to decline suspicious EMV® fallback transactions.

You’ll need to register, so look for the invitations the first week of August. On Aug. 8, 2016, the presentation slides will be available for you in the Fraud Watch section of SHAZAM Access.

Prepare your questions now, as we’ll allow time at the end to answer as many as we can!

For more information

If you have any questions about our biannual webinar, please call SHAZAM fraud operations at 800-537-5427, ext. 2899.
Reminders when using SHAZAM Card Block

SHAZAM Card Block is an important and effective tool in dealing with fraud. It allows your financial institution to block fraudulent transactions based on state and merchant category code, dollar amount, country, etc.

**Using transaction blocking**

MasterCard® and Visa® both support the use of transaction blocking to avoid and reduce fraud losses. It's important to remember that under no circumstance should bank identification number (BIN)-level blocks be implemented as a way to control how the cardholders can or can't use their card. In most cases, you can control the fraud by simply blocking SHAZAM® Chek (non-PIN) activity. So, if your cardholder uses their PIN, they wouldn't be affected by the BIN block.

If your financial institution uses SHAZAM Card Block at a BIN level to address current fraud trends, you don’t need to notify your cardholders. However, it’s recommended that you incorporate language or after-hours recordings on your home banking site that:

- Advises cardholders you may have blocks
- Isn’t too specific about the blocks (in order to avoid unwanted access)
- Tells cardholders to use their PIN whenever possible

Following these steps can help cardholders avoid any inconvenience when making their valid transaction.

**Please Note:** If you receive a call from a cardholder that’s unable to complete a valid transaction due to a BIN-level block, your financial institution will need to perform a PAN block or primary account number (PAN) exclusion to allow the cardholder’s valid activity.

**Proactive block**

A proactive block, such as blocking all non-U.S. countries, requires a 30-day notice to your cardholders letting them know of the action you’re taking. In the notice, you must advise your cardholders that if they want to use their card overseas — whether they’re traveling or trying to make an internet purchase — they can call you and you’ll make adjustments to allow their valid purchases.

**For more information**

If you have any questions about using SHAZAM Card Block, please call SHAZAM fraud operations at 800-537-5427, ext. 2899.
New Easy PIN option: No reference numbers

Choose the solution that works best for you at the BIN level

We’re pleased to share that we’ve added a third option to SHAZAM Easy PIN®, our solution for offering customer-selected PINs. We’ve developed this user-friendly option to help further meet you and your cardholders’ needs.

The new option doesn’t require financial institutions to generate a reference number, which eliminates the need for separation of duties between staff members. Plus, this option uses cardholder information already known by the system for authentication.

You’ll find more information about all SHAZAM Easy PIN options and how to determine bank identification number (BIN) eligibility in the tables below. We understand one SHAZAM Easy PIN option may not fit your business needs, so you can choose the solution that works best for you at each BIN.

---

### New option now available: Without reference number

- Uses cardholder information already known by the system for authentication (PAN, last four digits of Social Security number, expiration date, CVV2 / CVC2).
- Cardholder must have the physical card before he or she calls and selects a PIN or activates the card.
- Financial institution doesn’t need to issue any reference numbers, which eliminates the need for separation of duties between staff members.
- Cardholder has the option to activate his or her card and change the PIN in one convenient call.
- Cardholder must call from a telephone number already on file.

### Reference number, plus last four digits of the PAN

- Cardholder needs reference number and last four digits of the PAN to complete a PIN selection.
- Financial institution performs plastics maintenance and associates the reference number with the PAN before the cardholder can call and select a PIN.
- Cardholder calls a separate interactive voice response (IVR) system for card activation.
- Cardholder doesn’t have to call the IVR system from a specific telephone number.

### Reference number only

- Cardholder only needs a reference number to complete a PIN selection.
- Cardholder calls a separate IVR system for card activation.
- Cardholder may perform PIN selection before the financial institution performs plastics maintenance.
- Cardholder doesn’t have to call the IVR system from a specific telephone number.

---

1 Financial institution must have plastics on file with SHAZAM
2 SHAZAM must perform your PIN verification to be enrolled in one of the SHAZAM Easy PIN options
3 SHAZAM must have CVV2 / CVC2 keys on file

---

– Continued on next page
Easy PIN – Continued from previous page

**Take note**
The new SHAZAM Easy PIN option without a reference number is more user friendly for your financial institution to administer. However, the use of a reference number provides the financial institution with an added level of control and security. Be sure to consider the available options carefully and choose the option that best meets your business needs.

---

**Enrollment**
Interested in moving to the new SHAZAM Easy PIN No Reference Number option? Simply complete the SHAZAM Easy PIN Request Form and email it to customerimplementation@shazam.net or fax it to 800-267-0549.

Requests for adding SHAZAM Easy PIN will be handled on a first-come, first-served basis. A SHAZAM project manager will contact you regarding the implementation as soon as possible.

**Free plastics report**
Want to enroll but feel your database needs some additional work to prepare? Simply ask your SHAZAM project manager for a free plastics report ($100 value) that you can use to identify and make changes prior to your implementation.

**Learn more**
We encourage you to look at all three options for SHAZAM Easy PIN, and we’d be happy to discuss more about this product with you. If you have any questions about SHAZAM Easy PIN, please call SHAZAM client support at 800-537-5427 (option 2) or submit a service request online using SHAZAM® Web Rep.
Hackers know your vulnerabilities; do you?

SHAZAM successfully defends our own network from 3.5 million attacks each month. We can do the same for you!

Your firewall is the first line of defense against external threats. Managing this critical security element is a full-time commitment. Have SHAZAM Secure* experts monitor your internal and external threats, and let hackers know they’ve met their match. When you take advantage of managed firewall services, you can:

• Outsource your firewall protection at a very competitive price
• Feel secure in our expertise at defending our own network
• Free your staff 24/7 from intrusion detection / prevention monitoring and response
• Trust your firewall is properly provided, deployed, upgraded and patched on a continual basis
• Meet regulations requiring proof of managed firewall services

What we do for you

SHAZAM Secure provides monthly reports tailored to your financial institution. You’ll receive easy-to-read data regarding:

• Intrusions to your application layer
• TCP / IP anomaly events indicative of an attack
• Gateway virus detection and origination
• Internal web activity and blocked or filtered sites
• Detection and levels of data / virtual private network (VPN) usage

Start defending today

Defend your network with SHAZAM Secure. Contact Tom Quist, SHAZAM Secure account executive, at 800-537-5427, ext. 4370, to learn about the many advantages of SHAZAM Secure managed firewall services and sign up today.
New client support menu options

Check them out before calling SHAZAM

Effective Aug. 1, when you call SHAZAM, you’ll hear our new menu options for SHAZAM client support.

We’re updating these options to ensure you’re directed to the correct party the first time you call us. This update will also help lower the chances of transferring your call to another department, which may extend your call time.

Please distribute the updated SHAZAM client support menu options to your team members. We encourage you to print and place them by your telephones for reference when calling SHAZAM. The menu options can also be viewed and printed through SHAZAM Resource.

Please be aware that we’re only updating the menu options. Our main client support telephone number will remain as 800-537-5427.

For more information

If you have any questions, please call SHAZAM client support at 800-537-5427 or submit a service request online using SHAZAM, Web Rep.
Make life easier using SHAZAM Web Rep fraud forms

Did you know you can easily and quickly submit a SHAZAM case management travel notice or a FICO® Falcon® Fraud Manager real-time scoring exclusion form through SHAZAM Web Rep in SHAZAM Access? It’s true! Not only are the forms easy for you to complete online and secure to send, but you’ll also receive immediate confirmation that we’ve received your forms for processing.

In addition, forms are entered more quickly into the system. If you submit either of these forms by email or fax, each one has to be entered manually. We receive hundreds of these forms daily — that takes a long time!

When you submit the forms through Web Rep, they’re uploaded and automatically entered several times throughout the day. This allows your information to be entered more quickly and accurately as you choose state and country codes from drop-down menus.

As we continue to see the email and fax form submissions dwindle, you can expect that eventually we’ll only accept the forms through Web Rep. At this time, there’s not a set date, but we strongly encourage you to start using the Web Rep forms today.

**Falcon Real-time Scoring Exclusion Form**

This form allows you to exclude a cardholder / primary account number (PAN) from Falcon Real-time scoring for a period of time, preventing the PAN from receiving any Falcon Real-time declines (Action Code 102).

**SHAZAM Case Management Travel Notice**

This form puts a note within the Falcon case management system that will tell our fraud specialists where and when a cardholder will be traveling. We’ll only see this information if a Falcon case is created. When the case is worked, if the suspicious activity is in the same location as where you’ve told us the cardholder will be traveling, we won’t place a temporary card block on the account. We’ll make one attempt to contact the cardholder, and if we can’t reach him or her, the case will be closed as “Unable to Confirm.”

If the suspicious activity is occurring somewhere other than where the cardholder is traveling, a temporary card block may be applied.

**For more information**

If you have any questions, please call SHAZAM fraud management at 800-537-5427, ext. 2899.
Cardholders will show off custom debit cards; you’ll increase revenue

We all have that one picture that takes us back to an amazing time in our lives. It might be a wedding, an amazing vacation or a child scoring the winning point. Help your cardholders remember their favorite moment with a SHAZAM myPic Studio™ customized debit card.

Cardholders can personalize their debit card with a picture of their choice: family, friends, pets or the perfect vacation spot. The possibilities are endless!

Our campaigns

New SHAZAM myPic Studio campaigns are now available on SHAZAM Power Marketing. These three distinct campaigns encourage your cardholders to show off their favorite moments on a SHAZAM myPic Studio custom debit card.

Cardholders will also learn how easy it is to create a beautiful custom card they’ll be proud to use.

Want the new SHAZAM myPic Studio campaigns? Placing an order is easy — visit SHAZAM Power Marketing, click Card Usage, then myPic Studio and order your material today!

New to SHAZAM Power Marketing?

Create your new account by clicking Submit Registration. You’ll have instant access to our wide variety of marketing campaigns to meet your institution’s needs.

Forgot your password?

No problem. Click Forgot your password? located directly below the Returning Customers: Quick Login section. You’ll be asked to enter your email address for password assistance.

NEW

cardholders will
love showing off
their favorite
SHAZAM myPic Studio®
custom debit cards,
and you’ll increase
your revenue.

New Visa®
and MasterCard®
myPic campaigns are
now available!
Helpful tips for SHAZAM Access Files tab upgrade

In April, we updated the Files tab on SHAZAM Access, which provided a new look and feel, plus a few different procedures that had presented challenges for some users.

After hearing your concerns, we’ve compiled many tips below that will help you access and navigate the upgraded Files tab.

**Browser issues**

The new SHAZAM Access Files tab behaves differently in different internet browsers. Because Internet Explorer® is the preferred browser for SHAZAM Access, the instructions below apply only to Internet Explorer.

As a result of this upgrade, SHAZAM strongly encourages all financial institutions to save files first, which simplifies viewing and printing. We also recommend associating files to Microsoft® Word®.

**Changing a file association**

Use this procedure if you need to change the program used to open or save a file and you’ve already established a file association to a different program that’s not working for you. For example: changing the file association from Notepad to Word.

---

**SHAZAM recommends associating files to Microsoft Word.**

1. Navigate to the Start menu and choose Default Programs.

2. Select *Associate a file type or protocol with a program*.

3. Locate the file extension with the report ID you want to change. **Please Note:** The file extension is the same as the report ID you want to change. For example: .ssr110 or .ssr120.

4. Select the report name and click *Change Program…*

5. Select Word or another preferred program from either Recommended Programs or Other Programs. **Please Note:** You may have to click the down arrow under Other Programs to view all options.

6. Click the checkbox next to the *Always use the selected program to open this kind of file* message, then click OK.

---

–Continued on next page
**Saving and printing files**

1. Select the files you want to save (you can select as many as you like).
2. Click **Save to Zip File**.
3. Click **Save** on the Open or Save prompt.
4. Click **Open** on the next prompt. A WinZip window will appear. **Please Note:** If you’re saving multiple reports to the same directory, press Ctrl+A to select all reports within the WinZip window.
5. Right-click on the file or files and choose **Extract**.
6. Navigate to the folder where you want to save the files.
7. Click **Unzip**.
8. If you’ve associated a file to Word and you want to print one or more individual reports, right-click on the report, select **Open With** and select **Internet Explorer**. This won’t change your file association. **Please Note:** See the Changing a File Associations section if you want to change the file type used for a specific file.
9. Click the **Print icon** to print your report.

**Viewing files**

1. Viewing files can be accomplished in the following manners:
   - Right-clicking the file and choosing **Open in browser**
   - Double-clicking on the file

**Creating a file association**

You’re required to create a file association the first time you view a saved report.

1. Double-click the file to open.
2. Choose **Select a Program from a List of Installed Programs**, then click **OK**.
3. Choose Word or another preferred program from either Recommended Programs or Other Programs. **Please Note:** You may have to click the down arrow under Other Programs to view all options.
4. Click the checkbox next to the **Always use the selected program to open this kind of file** message, then click **OK**.

**Please Note:** Reports shouldn’t be associated to PDF.

**Questions?**

Please call SHAZAM client support at 800-537-5427 (option 2) or submit a service request online using SHAZAM’s Web Rep.
SHAZAM training

SHAZAM Debit Card Fraud and Chargebacks seminar

**Sept. 14: Memphis, Tennessee**
DoubleTree – Memphis Downtown
185 Union Ave.
901-528-1800

**Sept. 28: St. Louis, Missouri**
Hilton Downtown
400 Olive St.
314-436-0002

**Description:** Learn everything you need to know about debit card fraud, disputes and chargebacks. Topics include:

- Fraud trends
- Risk management tools
- Fraud reporting
- The complete chargeback cycle, including:
  - Retrieval requests
  - Chargeback reasons
  - Financial institution and merchant responsibilities
  - Documentation

---

**September 2016**

<table>
<thead>
<tr>
<th>Sun</th>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thu</th>
<th>Fri</th>
<th>Sat</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
</tr>
<tr>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
</tr>
<tr>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
<td>29</td>
<td>30</td>
<td></td>
</tr>
</tbody>
</table>

**SHAZAM Settlement Process and Reporting webinar**

**Sept. 8:** 9:30–11:30 a.m. CT
**Sept. 20:** 1:30–3:30 p.m. CT

**Description:** The settlement process is an important part of your ATM or debit card program. This two-hour webinar will explore how the SHAZAM settlement process works and will give you insights on how to effectively manage the settlement process. You’ll also learn how settlement affects your institution and why your institution receives daily reports from SHAZAM.

For more details on training events, visit our [Training Services](#) page.
‘Pampered Rewards’ winners

Congratulations to our grand prize winner, Cindy W. of Davenport, Iowa. Cindy won a $500 Spafinder gift card in the “Pampered Rewards” Debit Rewards campaign, which ran April–June 2016. Cindy is a customer of the R.I.A. Federal Credit Union in Milan, Illinois.

We’d also like to congratulate our June monthly winners listed at right, who each received a $50 relaxation gift card.

June winners

- Andrew R. of Albertville, Minnesota (Financial Security Bank; Kerkhoven, Minnesota)
- Lindsay S. of Des Moines, Iowa (Freedom Financial Bank; West Des Moines, Iowa)
- Danielle G. of Garner, Iowa (Reliance State Bank; Story City, Iowa)
- Matthew M. of Trumann, Arkansas (Southern Bancorp Bank; West Helena, Arkansas)
- John M. of Topeka, Kansas (Equity Bank; Wichita, Kansas)
- Wesley S. of Pleasanton, Kansas (Labette Bank; Parsons, Kansas)
- Ashley B. of St. James, Missouri (The Maries County Bank; Vienna, Missouri)
- Ronnie H. of Pinckneyville, Missouri (First National Bank in Pinckneyville; Pinckneyville, Illinois)

About the newsletter

Spotlight on Service, winner of 15 awards of publication excellence, provides you with information on the financial services industry. It’s not a definitive analysis of the subjects discussed and is not an alternative to the requirements of any regulatory agency.

To join the Spotlight on Service subscription list, send us your name, account number and email address. We also welcome your questions or comments about the newsletter.