Consumer End-User Safety & Security FAQs

1. What is a faster payment?	The term "faster payments" is broadly used in the payment industry to indicate simply that increased speed, convenience, and accessibility are essential features for the future of the payment settlement system. In addition to the expedited movement and availability of funds, the more efficient and transparent provision of information about the transaction is a key component of the faster payments value proposition. **Immediate** - can be sent 24 hours a day, seven days a week (subject to the service offering of the financial institution) and receives a response to the sending bank within 15 seconds, confirming that the receiving bank has accepted or rejected the payment **Instant** – an electronic retail payment solution available 24/7/365, resulting in the immediate or close-to-immediate interbank clearing of the transaction and crediting of the payee's account with confirmation to the payor (within seconds of payment initiation) **Same Day** – a payment for which the effective entry date is the same as the date on which the entry was initiated by the sender *Source – Faster Payments Playbook https://fasterpaymentsplaybook.org/ To date, the industry has used the terms faster, real-time, and instant payments as if they were interchangeable. However, different networks offer options that differentiate among those terms based on how fast the transactions post to your account and when the funds actually arrive. We believe the following terms are more descriptive and helpful: • Faster Payment: Within 24 hours, the recipient receives notification of the payment and has access to good funds obtained from the sending account. • Instant Payment Notification: Within 60 seconds, the recipient receives notification of the payment, but access to good funds obtained from the sending account may not occur for

		up to 24 hours (the receiving financial institution may provide good funds access prior to obtaining funds from the sending account). • Instant Payment: Within 60 seconds, the recipient receives notification of the payment and has access to good funds obtained from the sending account. Because the funds move so fast in and out of it is important to know what rules your payment service provider follows regarding reversing transactions sent in error. Use these methods to send funds only to people and entities you know and trust.
2. What should I consider before making a faster payment versus a more traditional payment?		It is possible that you will not be able to stop the payment, so only pay people and entities you know and trust after confirming that you are sending the money to the correct party. Make sure you understand how much you will be charged for the transaction and any associated fees. Be aware that the funds will come out of your account immediately. Once you have considered these things you may find that because funds are immediately available to the individual or company to whom you're sending a payment, faster payments can be beneficial for transactions such as paying a bill on the day that it is due or sending money to another person right away. However, additional fees may be assessed, and depending on the faster payment service used, you may not be able to revoke or cancel the transaction after it has been initiated/approved. It is important to review the terms and conditions before initiating a payment so that you can choose the payment method that fits your particular circumstance.
3. What should I do to keep my account safe?		There are several practices that you can follow to help keep your financial account safe. These practices are helpful regardless of the type of payment you might initiate from the account. Passwords: Do not use words that are easy for someone to guess based on knowing you (e.g., children's or pet names) or that would be easy to guess based on social media profiles (such as birthday or hometown). Do not give your password to anyone, even to family or friends, and especially do not provide your password to anyone that contacts you by telephone or email who

		claims that they are from your financial institution. Legitimate organizations such as your financial institution or a government agency like the IRS or Social Security Administration will NEVER email you or phone you and ask for your password. Layered Security: In addition to setting a complex password and keeping it private, you should understand that layered security provides additional protection. Multi-factor authentication is offered by most financial institutions, and it allows you to set up an additional step besides your login and password in order to access your financial information. For instance, you can provide a mobile number, and once you enter your name and password, your financial institution will text or call you with a one-time password that is also required before you can get into your account. Multi-factor authentication processes have been proven to be safer because a fraudster would have to be able to unlock your phone before accessing your account, which is far less likely than simply breaking a password online. Virus Protection: Update your virus protection software on any device you use to access your banking services. WiFi: Use secure networks only. Do not access your bank account or make a payment while connected to a public WiFi system, such as the free WiFi systems available in a coffee shop, airport, etc. Monitoring: Keep track of your bank account regularly. Take advantage of 24x7 accessibility to your bank account via the Internet or smart phone to frequently and consistently monitor transactions. If you see something unusual or unexpected, contact your financial institution immediately. Trusted Party: Only use a faster payment system to pay people you know and trust. If you are paying someone you know and trust, verify that you are sending the money to the correct person you want to pay. And, make sure that you know that the person is who they say they are. Faster payments may have unique qualities that differ from other types of payment methods, such as the inability to cancel or revoke a faster payment transaction once it has been initiated.

	The Federal Trade Commission has additional resources online about how to keep your personal information safe: https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure
4. What consumer protections are in place for my account?	The best source of information about specific protections is your payment service provider. Another source of information is the CFPB "Bank accounts and services" web page.
5. When it comes to safety/security, how are faster payments different than more traditional payments?	Faster payments can be as safe as or safer than a traditional payment, provided you follow basic safety procedures to keep your information secure, such as the tips included in this document. If you are using faster payments to transfer money directly person to person (P2P), you must have the correct information about the person to whom you are sending money. Confirming the email or mobile number or other identifier associated with the person you are paying prior to sending a payment is critical to ensuring the right person will receive the money. While some P2P services have protections in place that allow for refunds of unauthorized or mistaken transactions, protections differ across services. Some P2P programs have a registry that requires participants to enroll in order to use that service. While this may allow you to select your contacts more readily, you should always confirm the information of a recipient before sending a payment.
6. What should I do if I lose my device that was set up to make faster payments?	Contact your financial institution first to let them know that your account may be compromised. Then contact your service provider to see if they can erase the content or block access to the lost device.
7. What should I do if I accidently sent a payment to the wrong person?	Some faster payments solutions will have a "pending" status once you initiate a transaction. During the "pending" period, you may be able to cancel the payment. If the payment has already been completed and the money has been moved from your account, your financial institution may be able to help get your money back. However, it is important to familiarize yourself with the terms, conditions and protections of any faster payment service before you use it.

8. What should I do if I see a faster payment transaction on my account that I did not authorize?	Report it to your financial institution immediately. If you do not contact your financial institution in a timely manner, you may not be able to recover the money. It is best to contact your bank in person or over the phone, and then follow up in writing, if your financial institution requests, sent to the address your financial institution gives you, along with a copy of all papers you have related to the unauthorized payment. Keep a copy of all papers for yourself. You should also check your bank statement every month to look for unauthorized payments out of your account.
9. What should I do if I unexpectedly receive funds into my account from someone I do not know?	Report it to your financial institution immediately. **Do not spend the money, as you may be required to return the funds**.
10. What should I do if I sent a payment and I didn't receive the goods in exchange?	The protections for faster payments solutions vary, and some do not allow transactions to be reversed or canceled once the payment is authorized. Faster payment solutions should only be used to send funds to people and entities you know and trust. For example, avoid using faster payments in conjunction with online purchases, or for football or concert tickets that can be easy targets for scammers. If this does happen, contact the recipient of the money to resolve the problem directly. If the issue isn't resolved to your satisfaction, notify your financial institution.
11. How can I verify that the person I am sending money to is really who they say they are?	You should only use faster payments to send money to people and entities you know and trust. Before you complete the transaction, confirm the email address, phone number or other identifier is correctly associated with the recipient. The particular faster payment network may offer methods to ensure that the recipient is who they say they are.
12. What should I do if I realize that I was scammed into authorizing a payment to	You should only use faster payments to send money to people and entities you know and trust. Unfortunately, if you fall victim to one of those scams, there isn't much that your financial institution will be able to do. You should still contact your financial institution, which can report

someone (e.g., African Prince, lottery winnings, help your grandchild in trouble, etc.)?		the fraud and may be able to help you file a complaint to attempt to get your money back, though there is no guarantee. You should also consider reporting the fraud to the FTC, your state attorney general's office, or the police. Various government agencies such as the Federal Trade Commission and the Federal Bureau of Investigation have resources online to warn consumers of various online and telephone scams: https://www.consumer.ftc.gov/features/scam-alerts https://www.fbi.gov/scams-and-safety/common-fraud-schemes
13. Who do I contact when there is a problem with a mistake with a payment or fraud?		Contact your financial institution as soon as you realize there is a problem. You can find that contact information on a bank's online banking application or website.